✓کارنیل، بزرگترین شبکه موفقیت ایرانیان می باشد، که افرادی زیادی توانسته اند با آن به موفقیت برسند، فاطمه رتبه ۱۱ کنکور کارشناسی، محمد حسین رتبه۶۸ کنکور کارشناسی، سپیده رتبه ۳ کنکور ارشد، مریم و همسرش راه اندازی تولیدی مانتو، امیر راه اندازی فروشگاه اینترنتی،کیوان پیوستن به تیم تراکتور سازی تبریز، میلاد پیوستن به تیم صبا، مهسا تحصیل در ایتالیا، و..... این موارد گوشه از افرادی بودند که با کارنیل به موفقیت رسیده اند، شما هم می توانید موفقیت خود را با کارنیل شروع کنید.

برای پیوستن به تیم کارنیلی های موفق روی لینک زیر کلیک کنید.

www.karnil.com

همچنین برای ورود به کانال تلگرام کارنیل روی لینک زیر کلیک کنید.

https://telegram.me/karnil

بسمه تعالی

مجموعه مقالات همایش

بررسی ابعاد حقوقی فناوری اطلاعات

Seminar On
The Legal Aspects *of* Information Technology
Proceeding

تهران – خرداد ۱۳۸۳
کمیته مبارزه با جرایم رایانه‌ای
مرکز مطالعات راهبردی و توسعه قضایی

Iranian Cybercrime Committee
Published: June 2004

شناسنامه همایش

مجری: کمیته مبارزه با جرایم رایانه‌ای

دبیر همایش: رضا پرویزی

زمان برگزاری همایش: خردادماه ۱۳۸۳

آدرس وب سایت: www.itlawseminar.net

آدرس پست الکترونیک همایش: info@itlawseminar.net

اعضای کمیته علمی:

دبیر کمیته علمی: رضا پرویزی

دکتر علیرضا جمشیدی
دکتر امیر صادقی نشاط
دکتر ستار زرکلام
دکتر عبد الصمد خرم‌آبادی
دکتر محمد علی اردبیلی
دکتر علی حسین نجفی ابرندآبادی
مهندس محسن ابوالقاسمی
دکتر فیضی چکاپ

اعضای کمیته اجرایی:

مدیر اجرایی همایش: مهندس علیرضا کاشیان

مسوول دبیرخانه: حمیدرضا خانی اوشانی

تدارکات: حمیدرضا عطایی

امور مالی: احمد صارمی

روابط عمومی: سیروس لطفی

امور گرافیک: سعید اخوان قربانی

امور تشریفات: شاهپور دولتشاهی

امور تایپ: ستاره امیر اصلانی

خبرخوانی مقالات: ایمان هاشمی

جهت دریافت مجموعه مقالات با آدرس پست الکترونیک همایش مکاتبه نمایید.

فهرست مقالات

☑ عنوان: مقدمه

☑ نویسنده: رضا پرویزی (دبیر همایش)

دنیایی که امروزه در آن زندگی می‌کنیم، با پا گذاشتن به هزارهٔ سوم میلادی تحولات بسیار سریع و شگفت‌آوری را در تمام شؤون خود تجربه می‌کند. بدون شک یکی از عوامل مهم و عمدهٔ این تحولات فن آوری اطلاعات می‌باشد.

ویژگی برجسته فن‌آوری اطلاعات، تاثیری است که بر تکامل فن‌آوری ارتباطات راه دور گذاشته و خواهد گذاشت . ارتباطات کلاسیک هم‌چون انتقال صدای انسان، جای خود را به مبادله مقادیر وسیعی از داده‌ها، صوت، متن، موزیک، تصاویر ثابت و متحرک داده است. این تبادل و تکامل نه تنها بین انسانها بلکه ما بین انسانها و کامپیوترها و همچنین بین خود کامپیوترها نیز وجود دارد.

در نتیجه این تحولات، جامعه‌ای مجازی با آثار واقعی پدید آمده است. جامعه‌ای که تمامی فعالیت‌های اجتماعی، اقتصادی، سیاسی و هنری را به‌طور شگفت‌انگیزی تحت تاثیر قرار داده و مبادلات تجاری، تعامل بین حاکمیت و شهروندان، توزیع اطلاعات علمی، هنری، آموزشی و خلاصه همه نهادهای جدید عصر صنعتی از آن متاثر گشته است. تحولات جدید موجب غیر مادی شدن واسط انتقال اطلاعات شده که در نتیجه باعث:

۱. حذف حضور فیزیکی افراد،
۲. حذف واسطهای مادی انتقال اطلاعات مثل کاغذ و پلاستیک
۳. حذف تقریبی مدت انتقال اطلاعات و نهایتا
۴. پیدایش محیط مجازی با ویژگیهای خاص خود می‌شود.

همچنین ارزشهای جدید و آسیب‌پذیری مانند ۱- محرمانه ماندن اطلاعات: حفظ اطلاعات در برابر افشای غیرمجاز آنها (confidentiality)[۱] ۲- تمامیت اطلاعات: حفظ صحت اطلاعات در برابر تغییر یا آسیب به آنها (integrity)[۲]

۱- این عامل باعث می‌شود تا کسانی که هیچگونه مجوزی ندارند یا اجازهٔ آنها به اندازه‌ای نیست که بتوانند از آن اطلاعات استفاده کنند، از دسترسی به آن اطلاعات منع شوند. در حقیقت تعرض به این عامل، تجاوز به حقوق مشروع دیگران مبنی بر حفظ اطلاعات شخصی و خصوصی آنها می‌باشد. از آنجا که هتک سیستم دیگری و ورود به آن سرمنشاء تمامی راههای کسب نامشروع اطلاعات می‌باشد، بسیاری بر این عقیده‌اند که تعرض به این عامل، اصلی‌ترین و مهمترین جرم در گروه جرایم کامپیوتری محسوب می‌شود. تعرض به این عامل عموما زمانی به وقوع می‌پیوندد که یک متعرض (هکر) اطلاعات کاربر یا آنچه را که متعلق به او می‌باشد را بدون اجازه مشاهده یا کپی نماید.

۲- این اطمینان را بوجود می‌آورد که هیچ کس بدون داشتن مجوز حق ندارد به اطلاعات دست یافته و تغییری در آنها بوجود آورد. بنابراین هرگونه مزاحمت و خسارت یا تغییر در اطلاعات ثبت شده در کامپیوتر یا قسمتهای دیگر آن، بدون مجوز قانونی موجبات تعدی و تجاوز به این عامل مهم در تبادل اطلاعات الکترونیکی را فراهم می‌آورد. بسیاری از تعرضات عمدی که توسط هکرها صورت می‌گیرد مانند وارد کردن ویروسهای کامپیوتری از قبیل worms و Trojan horses در این رده جای می‌گیرند. این امر نه تنها از جانب کسانی که منافع اقتصادی را دنبال می‌کنند به وقوع می‌پیوندد، بلکه آنهایی که قصد مقابله به مثل (انتقام)، اغراض سیاسی، تروریسم یا صرفا قصد رقابت داشته باشند نیز مرتکب می‌شوند.

۳- موجودیت اطلاعات و خدمات: حفظ عملکرد مفید سیستم و در دسترس نگهداشتن اطلاعات (availability)[۳] را برای جامعه و افراد ایجاد می‌کند که نیازمند حمایت جدی می‌باشند.

فن‌آوری اطلاعات با تمام قابلیتها و پیچیدگیهایش به شدت در مقابل تهدیدات آسیب پذیر است. بدین ترتیب که فن‌آوری اطلاعات ارتکاب اعمال مجرمانه‌ای را که پیش از این به هیچ وجه امکانپذیر نبود فراهم نموده است. سیستم‌های کامپیوتری فرصت‌هایی تازه و بسیار پیشرفته برای قانون شکنی در اختیار مجرمین می‌گذارند و توان بالقوه ارتکاب گونه‌های مرسوم جرایم را به شیوه‌هایی غیر مرسوم به‌وجود می‌آورند. تهدیدات علیه جامعه اطلاعاتی را جرم کامپیوتری یا جرایم مرتبط با کامپیوتر می‌نامند.

آسیب‌پذیری امروزی جامعه اطلاعاتی از جانب جرم کامپیوتری تا کنون به درستی و بطور کامل مورد تجزیه و تحلیل قرار نگرفته است. تجارت و بازرگانی، امور اداری و در مجموع جامعه ما بر کارآیی و امنیت بسیار بالای فن‌آوری مدرن اطلاعات استوار است. مثلا در جامعه تجاری بسیاری از معاملات پولی بوسیله کامپیوترها و در غالب سپرده‌گذاری انجام می‌شود. در تجارت الکترونیک برای انجام معاملات پولی در شبکه‌های کامپیوتری به سیستم‌های امن نیاز می‌باشد. کل تولید یک شرکت به عملکرد سیستم پردازش داده آن وابسته است. بسیاری از تجار، اطلاعات و اسرار تجاری با ارزش خودشان را بصورت الکترونیکی ذخیره می‌کنند. سیستم‌های کنترل هوایی، دریایی و فضایی و همین‌طور پزشکی تا اندازه زیادی متکی بر سیستم‌های کامپیوتری هستند. کامپیوترها و اینترنت نقش کلیدی در آموزش و تعلیم و تربیت خردسالان دارند. شبکه‌های کامپیوتری بین‌المللی به منزله سلسله اعصاب اقتصاد، بخش عمومی و جامعه هستند. امنیت این سیستم‌های کامپیوتری و ارتباطی و مراقبت از آنها در مقابل جرایم کامپیوتری از اهمیت ویژه‌ای برخوردار است.

لذا به منظور آشنایی کاربران و متخصصین فن‌آوری اطلاعات و همچنین حقوقدانان با ابعاد مدنی و کیفری فن‌آوری اطلاعات، همایشی تحت عنوان بررسی ابعاد حقوقی فن‌آوری اطلاعات با مساعدت دبیرخانه شورای عالی اطلاع‌رسانی و دبیرخانه شورای عالی توسعه قضایی برگزار گردیده است.

لازم است از جناب آقای مهندس نصرالله جهانگرد و آقای دکتر علیرضا جمشیدی دبیران محترم شوراهای مذکور تشکر و قدردانی نمایم.

رضا پرویزی
دبیر همایش

۳- بیانگر این مطلب است که تحصیل اطلاعات و برنامه‌های مرتبط با آن از طرف یک کاربر، آن هم زمانی که بدان احتیاج دارد، نشانگر مفید و کاربردی بودن آنها است. نقض این عامل زمانی بوقوع می‌پیوندد که کاربر دارای مجوز برای مدتی از ارتباط مستمر و قابل اتکاء و اطمینان خود با سیستم و مرکز مورد نظر خود باز می‌ماند و از آن منع می‌شود. نمونهٔ بارز و معمولی که در این رابطه به وقوع می‌پیوندد denial of service attack می‌باشد. عملی است که به موجب آن از فعالیت عضو انجمن سیستمهای اطلاعاتی (AIS) مطابق با اهدافی که برای آن پیش بینی شده، جلوگیری می‌کند. این عمل ممکن است شامل جلوگیری از ارائهٔ سرویس یا فرایندهای محدود شده‌ای به سیستم میزبان شود. با اینحال این اصطلاح اغلب دلالت بر فعالیتهایی علیه یک میزبان یا یک گروه از آنها دارد که باعث غیرفعال شدن آنها در زمینهٔ ارائهٔ خدمات به کاربران خصوصا در ارتباط با شبکه می‌باشد.

☑ عنوان: تاریخچه، تعریف و طبقه‌بندی جرائم رایانه‌ای

☑ نویسنده: عبدالصمد خرم آبادی

(دادیار دیوانعالی کشور، دانشجوی دکترا حقوق جزا و جرم شناسی دانشگاه تهران)

مقدمه

برخی از مصنوعات بشری که دارای آثار عمیق در زندگی اجتماعی و اقتصادی انسان بوده حقوق خاص خود را ایجاد کرده‌اند. رایانه نیز یکی از مصنوعات بسیار مهم و منحصر به فرد بشری است که همه ابعاد زندگی انسان را دگرگون کرده و آثاری گسترده و شگرف به جای گذاشته است.

در ابتدای ورود رایانه به زندگی انسان تنها بخش‌های خاصی از جامعه تحت تأثیر آن قرار گرفته بود؛ ولی درسال‌های اخیر انقلاب فناوری اطلاعات به طور بنیادین جوامع را درکلیه زمینه‌های اقتصادی؛ اجتماعی؛ فرهنگی و سیاسی دستخوش تغییر و تحول نموده است به نحوی که اکنون به سختی می‌توان بخشهایی ازجوامع توسعه یافته را پیدا کرد که تحت تأثیر آن قرار نگرفته باشد.

انقلاب فناوری اطلاعات مرهون سه عامل است: ۱- موفقیت در توسعه و پیشرفت سیستم‌های کامپیوتری ۲- همگرائی بین سیستم‌های کامپیوتری و مخابراتی ۳- پذیرش و کاربرد گسترده و جهانی آن درتمام جنبه‌های زندگی و تمام رشته‌ها و مشاغل.

در یک دهه اخیر تعداد زیادی ازسیستم‌های رایانه‌ای جدید در اندازه‌های کوچک با ظرفیت پردازشی و ذخیره‌سازی بالاو هزینه نازلتر از گذشته در اختیار کاربران در رشته‌های مختلف قرار گرفته و قابلیت پردازش و ذخیره‌سازی هر نوع اطلاعات از قبیل متن؛ صوت؛ تصویرهای ثابت و متحرک در این سیستم‌ها موجب پیشرفت و استفاده بسیار گسترده از فناوری اطلاعات گردیده است. از طرفی همگرایی بین سیستم‌های کامپیوتری و مخابرات موجب پیشرفت و تکامل فناوری اطلاعات گردیده وتأثیر زیادی نیز بر تکامل فناوری ارتباطات راه دور گذاشته است در اثر این همگرایی ارتباطات کلاسیک همچون انتقال صدای انسان جای خود را به مبادله مقادیر وسیعی از داده‌ها مانند متن و صوت و تصاویر ثابت و متحرک داده است. این تبادل نه تنها بین انسانها بلکه بین انسان و رایانه و همچنین بین خود رایانه‌ها نیز وجود دارد. حالادیگر توانایی یا عدم توانایی برقراری یک ارتباط مستقیم چندان حائز اهمیت نیست بلکه کافی است که داده‌ها وارد شبکه‌ای شوندکه در آن آدرس فرستنده و مقصد هر فردی که قرار است داده‌ها در اختیار وی قرار گیرد مشخص باشد تا آنها بتوانند به داده‌ها دسترسی پیدا کنند. استفاده وسیع از پست الکترونیک و دستیابی به اطلاعات از طریق وب سایت‌های متعدد در اینترنت نمونه‌هایی از این پشرفت‌ها می‌باشدکه جامعه را به طرز پیچیده‌ای دگرگون ساخته است.[۱]

۱- ر.ک. گزارش توجیهی توصیه‌نامه R(۹۵) شورای اروپا (۱۹۹۵)

الف) آثار فناوری اطلاعات در زندگی انسان

امروزه نظام اداری کشورهای توسعه یافته با استفاده از فناوری اطلاعات اقدام بـه تشـکیل دولـت الکترونیـک نمـوده و از طریق اتوماسیون (خودکارسازی) نظام اداری و بهره‌گیری از سیستم اطلاعات مدیریتی، بوروکراسی و بسیاری از دیگر معضـلات اداری را که هزینه‌های هنگفتی بر جامعه تحمیل می‌کرد از بین برده است. نظام اقتصادی و تجاری با اسـتفاده از بـا نکـداری و تجارت الکترونیک و نظام فرهنگی با بهره‌گیری از نشریات وکتابخانه‌ها و موزه‌های الکترونیک و نظام آموزشی از طریق آموزش الکترونیک و تشکیل دانشکده‌ها و مؤسسات آموزش مجـازی، نظـام کشـاورزی، زمـین شناسـی، حمـل و نقـل، هـوا شناسـی، فضانوردی و امور نظامی و دفاعی از طریق استفاده از سیستم‌های اطلاعات جغرافیایی، نظام صنعتی و خدماتی، توزیـع آب، بـرق و گاز و خدمات بهداشتی درمانی از طریق استفاده از سیستم‌های کامپیوتری و شبکه‌های عمومی و خصوصی رایانه‌ای، از مزایای فناوری اطلاعات بهره‌مند گردیده و از طریق پیوند و همزیستی شگفت‌انگیز فناوری اطلاعـات بـا تمـام علـوم و فنـون گامهـای اساسی در جهت رفاه و آسایش انسانها برداشته شده و انجام بسیاری از مشاغل راحت‌تر گردیده است. آقای پرفسور زیبـر آلمـانی در کتاب حقوق کیفری اطلاعات می‌گوید: مهمترین قدرت تعیین کننده تغییرات حاصـله از پیشـرفت فنـاوری اطلاعـات گـذر از جامعه صنعتی به جامعه اطلاعاتی (فراصنعتی) است.این پیشرفت به حق، به وسیله جامعه شناسـان دومـین انقـلاب صـنعتی [یـا انقلاب فناوری اطلاعات] نامیده شده است. در حالی که خصوصیات اولین انقلاب صنعتی در طی قرن نوزدهم و بیستم جایگزین قدرت بدنی بشر به وسیله ماشین‌ها بود. ویژگی انقلاب دوم سوق یافتن فعالیت فکری بشر به ماشینها است.[۲]

ب) ارزش اطلاعات

در اثر انقلاب فناوری اطلاعات دارائی‌ها وامکانات غیرمادی مانند پول‌های جدید الکترونیک، مالکیت فکری، اسرار شغلی و دیگر اشکال فهم بشری به طور فزاینده واجد اهمیت شده است. اکنون اطلاعات نه تنها یک ارزش جدید بلکه عامـل قـدرت و یـک خطر بالقوه نیز شده است. وقتی که می‌گوییم اطلاعات یک ارزش جدید است به این معنی نیست کـه اطلاعـات قـبلاً ارزشـی نداشته است. در طول تاریخ بشر، خصوصاً از ابتدای دوران انقلاب صنعتی اطلاعات کالای با ارزشی بوده است. در آن روزهـای آغازین افراد دریافتند که هر کسی که اطلاعات خاصی را در اختیار داشته باشد انحصار سودمندی را به خود اختصاص می‌دهد و نسبت به کسانی که فاقد آن اطلاعات هستند در موضع قدرت قرار دارد، به همین لحاظ احتیاطهـای لازم بـرای حفـظ آن بـه عمل می‌آوردند. ابداع رایانه و تسهیلات ارتباطی پیش از آنکه مسائل جدیدی مطرح سازد ماهیـت مسـائل قـدیمی را دگرگـون کرده است. به طور سنتی پول کاغذی و مضروبات در صندوقخانه‌های فولادی و بتنی یا درهای دارای قفل رمزدار محفوظ نگـه داشته می‌شدند. امروزه بالاترین حجم پول به صورت الکترونیک درون سیستم‌های کامپیوتری ذخیره می‌شوند کـه صـندوقهای نوین به شمار می‌آیند. امروز اطلاعات هر جا و هر شکل باید به عنوان یک منبع و دارایی یک سازمان همانند پول واقعی یا مواد اولیه تلقی شوند. هر سازمانی در حال حاضر به طریقی می‌تواند یک کارخانه اطلاعات به شمار آید.[۳]

۲- زیبر اولریش جرم کامپیوتری و حقوق اطلاعات کیفری (جرائم کامپیوتری جلد دوم) ترجمه محمد حسن دزیانی، شورای عالی انفورماتیک، ص۱۳۲

۳- خبرنامه انفورماتیک ش ۵۲،ص۷۲،گروه بررسی حقوق مؤلفین نرم افزار- دبیرخانه شورای عالی انفور ماتیک

یکی از نویسندگان آمریکایی در کتاب خود به نام «جرائم سایبر» می‌نویسد:« امروز با ارزش‌ترین کالای جامعه ما گندم، فولاد و حتی فناوری نیست بلکه اطلاعات است. به دلیل وجود شبکه‌های رایانه‌ای هر کسی می‌تواند به گستره مبهوت کننده‌ای از اطلاعات دسترسی پیدا کند، در فضای سایبر هیچ مرزی وجود ندارد...»[۴]

ج) حقوق اطلاعات

تغییر ماهیت در مسائل قدیمی که به طور عمده به وسیله پیشرفت و توسعه فناوری اطلاعات ایجاد شده است موجب گردیده که در جامعه فراصنعتی اطلاعات تبدیل به یک کالای اقتصادی، اجتماعی، فرهنگی و سیاسی بسیار با اهمیت شود که نیاز به امنیت و نظام حقوقی مخصوص به خود داشته باشد.

بر همین اساس حقوقدانان تئوری حقوق اطلاعات یا حقوق فناوری اطلاعات را مطرح کرده‌اند وگفته‌اند: مقررات حقوقی مربوط به اطلاعات نمی‌توانند از طریق قیاس با مقررات موضوعات عادی بسط و گسترش یابد بلکه آ نها نیازمند مبنا وتئوری مستقل مختص خودشان هستند. وضعیت حقوقی قضائی کالاهای مادی و غیر مادی باید از هم متفاوت باشد و این تئوری اطلاعات را به عنوان یک عامل اساسی سوم در کنار ماده و انرژی ارائه و متحول می کند.[۵]

د) جامعه خطرناک

در خصوص امنیت در جامعه اطلاعاتی می‌توان گفت با توجه به این که عده‌ای فناوری اطلاعات را در اختیار اهداف شوم خود قرار داده‌اند جامعه اطلاعاتی با تمام پیشرفت‌ها و مزیت‌هایی که دارد، به شدت در مقابل خطرات و تهدیدات آسیب‌پذیراست، زیرا فناوری اطلاعات فرصت‌هایی تازه و بسیار پیشرفته برای قانون‌شکنی در اختیار مجرمین می‌گذارد و علاوه بر اینکه توان بالقوه ارتکاب گونه‌های مرسوم جرائم را به شیوه‌ای غیر مرسوم به وجود می‌آورد، ارتکاب اعمال مجرمانه‌ای را که پیش از این به هیچ وجه امکان‌پذیر نبود فراهم نموده است. بنابراین جرم رایانه‌ای به تهدیدی مهم علیه جامعه اطلاعاتی امروز تبدیل شده است. نفوذ فناوری اطلاعات به تمام ابعاد زندگی و همچنین تعامل و ارتباط میان کامپیوترها با شبکه‌های رایانه‌ای بین‌المللی، پدیده جرم رایانه‌ای را متنوع‌تر و خطرناکتر ساخته و بعد بین‌المللی به آن بخشیده است. بررسی و تجزیه و تحلیل جنبه‌های مختلف جرائم رایانه‌ای مشخص خواهد ساخت که کامپیوترهای مدرن و شبکه‌های ارتباطی دارای صفات و خصوصیاتی هستند که فرصتی بسیار مناسب برای مجرمین پدید می‌آورند و مشکلات بسیاری را فرا روی بزه‌دیدگان بالقوه و پلیس قرار می‌دهد. گروه‌های سازمان یافته جنایی فعال در سراسر جهان، جاسوسان صنعتی حرفه‌ای و سازمان‌های اطلاعاتی این امکانات و ابعاد جدید جرم کامپیوتری را در یافته‌اند، با این وجود، بسیاری از کشورها، تجار و کاربران عادی از حملات واقعی یا حملاتی که می‌تواند بر علیه آنها رخ دهد بی‌اطلاعند. در کتاب جرائم سایبر به نوشته‌های دو روزنامه‌نگار به نامهای دیویدفرید من [۶] و چالزمان [۷] اشاره شده که می‌گویند:«وزارت دفاع ایالات متحده بیش از ۲/۱ میلیون رایانه دارد (درسال ۲۰۰۰) که به حدود ۱۰۰۰۰

۴- جینادی آنجلیز، کتاب جرائم سایبر، فصل دوم ص ۲۲ ،ترجمه عبدالصمد خرم آبادی و سعید حافظی، سال ۱۳۸۲ شورای عالی توسعه قضایی

۵- زیبر اولریش- جرم کامپیوتری و حقوق اطلاعات کیفری جلد دوم کتاب جرائم کامپیوتری ترجمه دزیانی ص۱۳۵ و۱۳۴،سال ۱۳۷۶

۶- David Freed man

۷- Charles Mann

شبکه محلی پیوند خورده‌اند و این شبکه‌ها به یکصد شبکه راه دور متصل هستند. آنگونه که پنتاگون می‌گوید این شبکه‌ها در محاصره هکرها هستند. بر اساس داده‌های آژانس سیستم اطلاعات دفاعی[۸] در سال ۱۹۹۵ حدود ۲۵۰ هزار حمله به رایانه‌های وزارت دفاع انجام گرفته است. این آژانس معتقد است که در حدود دو سوم تلاش‌ها برای ورود به این رایانه‌ها موفقیت آمیز بوده و معمولاً کمتر از یک درصد آنها شناسایی شده‌اند. بسیاری از حمله‌ها به این سیستم نظامی خرابکاریهای جزئی بوده است. اما بعضی از آنها تنها یک حمله ساده نبوده‌اند. این آژانس پیش‌بینی می‌کند که تعداد حمله‌ها هر سال دو برابر شود. بر این اساس در سال ۱۹۹۷ شبکه‌های وزارت دفاع آمریکا هدف یک میلیون حمله قرار گرفتند. بنابراین جرایم سایبر تهدیدی جدی برای امنیت ملی خواهند بود[۹].

در اکتبر سال ۱۹۹۷ برق بیش از ۱۲۵۰۰۰ نفر در سانفرانسیسکو آمریکا قطع شده ممکن است در اثر خرابکاری کامپیوتری بوده باشد.نویسنده کتاب جرایم سایبر می گوید: اگر کرکرها با نیات شیطانی به رایانه های شرکت برق، آب، خدمات اورژانس، سیستم‌های ارتباط راه دور، بانکها یا هر سیستم حیاتی دیگر نفوذ کنند و ما می‌دانیم که بعضی از کرکرها این قابلیت را دارند، می‌توانند تمام جامعه را دچار هرج و مرج کنند.[۱۰] بنابراین فناوری اطلاعات نیز مانند سایر فناوری‌ها همان اندازه که در خدمت بشریت قرار گرفته و موجب رفاه و آسایش و پیشرفت او شده است تهدیدات و خطرات بالقوه‌ای نیز برای او ایجاد کرده است. به عبارت دیگر هر نوع فناوری به همان اندازه که مفید واقع می‌شود می‌تواند مضر هم باشد. به همین لحاظ جامعه شناسان و حقوقدانان از دهه ۱۹۸۰ به بحث از تصویر اجتماعی فناوری مدرن تحت عنوان و اصطلاح جامعه خطرناک پرداخته‌اند. اگر چه بیشتر این بحث‌ها بر خطرها و تهدیدهای ناشی از انرژی اتمی و مواد شیمیایی و مهندسی ژنتیک متمرکز بوده‌اند اما تجزیه و تحلیل و نتیجه حاصله از آنها می‌تواند در مورد فناوری اطلاعات نیز اعتبار داشته باشد. یکی از حقوقدانان اروپایی در این خصوص می‌گوید:«بیشترجامعه خطرناک در زمینه تکنولوژی اطلاعات رخ داده است. تغییرات کوچک داده‌ها می‌توانند مقادیر عظیم پول‌های پرداختی را موجب شود. مثلاً در تمام بانکها و یا سیستم‌های کنترل پرواز سابوتاژ (خرابکاری) کامپیوتری بر بیشتر بخشهای حیاتی اقتصاد مدرن اثر می‌گذارد. پیچیدگی و سرعت پیشرفت‌ها در حال رشد است. بدین ترتیب تعریف کلی و بحث برانگیز حقوق مختص جامعه خطرناک در مورد تکنولوژی اطلاعات نیز اجرا می‌شود.[۱۱]»

یکی از نویسندگان آمریکایی در این خصوص در کتاب جرایم سایبر نوشته است:«والتر لاکور[۱۲] یک متخصص تروریسم در مرکز مطالعات استراتژیک و بین‌الملل، می‌گوید که یک مقام رسمی سازمان سیا (سازمان جاسوسی آمریکا) ادعا کرده است می‌تواند با یک میلیارد دلار و ۲۰ هکر قابل ایالات متحده را فلج کند.لاکور یادآوری می‌کند که اگرچه هدف تروریستها معمولا قتل سران سیاسی و یا گروگان‌گیری یا بعضاً حمله ناگهانی به تسهیلات دولتی یا عمومی است، اما صدمه‌ای که ممکن است به وسیله حمله الکترونیک به شبکه‌های رایانه‌ای وارد آید می‌تواند بسیار غم‌انگیزتر باشد و اثر آن تا مدتها باقی بماند. لاکور معتقد است

۸- Defence Information System Agency

۹- جینادی آنجلیز جرائم سایبر، دبیر خانه شورای عالی توسعه قضایی، ترجمه عبد الصمدخرم آبادی و سعید حافظی، ص۳۸

۱۰- جینادی آنجلیز، همان،ص۴۱

۱۱- زیبر، اولریش، جرم کامپیوتری و حقوق اطلاعات کیفری، ترجمه محمد حسن دزیانی، جلد دوم جزوه جرائم کامپیوتری، دبیر خانه شورای عالی انفورماتیک، ص۱۳۶

۱۲- Walter Laqueur

که تروریسم رایانه‌ای ممکن است برای تعداد کثیری از مردم بسیار ویران کننده تر از جنگهای بیولوژیک یا شیمیایی باشد.»[۱۳]خطر و تهدیدات ناشی از جرائم رایانه‌ای به حدی است که دولت آمریکا یک تشکیلات به نام ستاد مسئول حفاظت از زیرساختها برای بررسی امکان حملات تروریستی الکترونیک علیه صنایع و خدمات حیاتی تشکیل داده است. اعضای آن عبارتنداند:

۱- اداره تحقیقات فدرال(F.B.I)
۲- سازمان جاسوسی آمریکا(C.I.A)
۳- سازمان امنیت ملی
۴- سیستم ارتباطات ملی
۵- وزارت دفاع
۶- وزارت انرژی
۷- وزارت دادگستری
۸- وزارت بازرگانی
۹- وزارت حمل و نقل
۱۰- وزارت دارائی

وظیفه این تشکیلات برنامه‌ریزی لازم برای جلوگیری از حملات رایانه‌ای به هشت زیرساخت به است که عبارتند از:

۱- ارتباطات راه دور (مانند شرکتها،مخابرات و رایانه های شبکه‌ای)
۲- سیستمهای الکتریکی (شرکتهای برق)
۳- تولید و ذخیره‌سازی و حمل و نقل نفت و گاز و بنزین
۴- سیستمهای بانکداری ملی
۵- حمل و نقل (مانند خطوط هوائی، راه‌آهن و بزرگراه‌ها)
۶- سیستمهای تأمین آب
۷- خدمات اورژانس
۸-خدمات دولتی که از طریق دولت الکترونیک ارائه می‌شود

نتیجه این که همه کشورهای جهان به نسبت میزان برخورداری و بهره مندی‌شان از فناوری اطلاعات در معرض خطرات و تهدیدات ناشی از این فناوری می‌باشند. قطعاً کشورهای توسعه یافته در حال حاضر به لحاظ استفاده بیشتر از این فناوری در معرض خطر بیشتری هستند. مثلاً دولت آمریکا چهار مرحله از پنج مرحله تشکیل دولت الکترونیک را پشت سر گذاشته است؛ در آن کشور و اکثر کشورهای اروپایی بسیاری از خدمات دولتی به صورت الکترونیک ارائه می‌گردد؛ فروشگاه‌های بزرگ که مراکز

۱۳- جیناذی آنجلیز، جرائم سایبر، ترجمه عبد الصمد خرم آبادی و سعید حافظی، جزوه دبیر خانه شورای عالی توسعه قضایی،۱۳۸۲، ص ۳۷

فروش الکترونیک نامیده می‌شوند کالاهای خود را از طریق شبکه‌های رایانه‌ای و به صورت مبادله الکترونیک به فروش می‌رسانند، در حالی که دولت ایران که از بسیاری از کشورهای در حال توسعه در این زمینه جلوتر است هنوز در مرحله اول تشکیل و تأسیس دولت الکترونیک می‌باشد و در سایر زمینه‌ها وضعیتی بهتر از این نداریم ولی ما نیز ناگزیریم این مسیر را طی کنیم.

ه)حقوق کیفری اطلاعات و وظیفه ما

کشورهای در حال توسعه نیز ناگزیرند که برای پیشرفت و توسعه کشور خود مجهز به فناوری اطلاعات شوند و طی کردن این مسیر اجتناب ناپذیر است و بدون بهره‌گیری از پیشرفته‌ترین فناوری نمی‌توان به توسعه و پیشرفت دست یافت، کسی که می‌خواهد در عصر فرا صنعتی و در جامعه اطلاعاتی زندگی کند باید خود را مجهز به پیشرفته‌ترین لوازم آن نماید. ترس از جرم نباید مانع از پیشرفت ما باشد. بقول یکی از اساتید حقوق دانشگاه میشیگان: «ما نمی‌توانیم با جنگیدن جلو پیشرفت فناوری اطلاعات را بگیریم و حتی نمی‌توانیم از آن فرار کنیم چرا که هیچ جایی برای فرار نخواهیم یافت که از این فناوری تأثیر نگرفته باشد پس تعلل و اتلاف وقت برای چیست ؟»[۱۴]

با توجه به آنچه که گفته شد ما نیز ناگزیریم که همگام با پیشرفت و توسعه کشورمان در زمینه فناوری اطلاعات برای مبارزه با تهدیدات و خطراتی که با آن مواجه هستیم برنامه‌ریزی کنیم و از تجربیات کسانی که این راه را قبل از ما طی کرده‌اند استفاده کنیم. اما تجربه دیگران نباید ما را به بی‌راهه تقلید کور کورانه بکشد. باید هر چه سریعتر تا دیر نشده است قوانین کیفری خود را بر اساس شرایط اقتصادی، اجتماعی، فرهنگی، سیاسی، حقوقی کشورمان روز آمد کنیم. اما فرا موش نکنیم که استفاده از راه حل حقوق جزا یعنی جرم انگاری و مجازا ت متخلفین نباید به عنوان تنها تدبیر برای کاهش خطرات و تهدیدات در جلوگیری از ارتکاب جرم و ایجاد امنیت در جامعه اطلاعاتی استفاده شود باید ضمن استفاده از تدابیر دیگر برخورد کیفری نیز به عنوان آخرین راه حل انتخاب شود. یکی از اساتید حقوق کیفری اطلاعات در این خصوص می‌گوید:«استراتژی جامع برای جلوگیری و کنترل جرم کامپیوتری تنها در تدابیر قضایی خلاصه نمی‌شود باید ترکیبی از موارد زیر را به اجرا گذاشت:

۱–تدابیر امنیتی اختیاری برای کاربران کامپیوتر

۲– تدابیر امنیتی (اجباری) توسط قوانین مر بوط به سخت افزار و نرم افزار

۳–آموزش و ارعاب مرتکبین بالقوه »[۱۵]

اتخاذ تصمیم صحیح و انتخاب راه حل درست در مورد یک موضوع منوط به داشتن شناخت دقیق از آن موضوع است و شناخت مشکلات و خطرات ناشی از فناوری اطلاعات لازمه انتخاب راه حل صحیح برای مقابله با آن مشکلات و خطرات است.

بررسی تاریخچه و تعریف و طبقه‌بندی جرائم رایانه‌ای گامی است در جهت شناخت تهدیدات و خطرات موجود در جامعه اطلاعاتی به منظور اتخاذ تدابیر شایسته. بنابراین ما این موضوع را در سه مبحث به شرح زیر مورد بررسی قرار می‌دهیم:

مبحث اول تاریخچه جرائم رایا نه‌ای.

مبحث دوم تعریف جرائم رایانه‌ای.

۱۴– افق یک، اطلاعات فناوری قضا، دفتر همکاری‌های فناوری ریاست جمهوری،۱۳۸۱، ص۲

۱۵– زیبر، اولریش، پیدایش بین‌المللی حقوق اطلاعات کیفری، ترجمه محمد حسن دزیانی، جزوه جرائم کامپیوتری،۱۳۷۶، ص۱۷

مبحث سوم طبقه‌بندی جرائم رایانه‌ای.

مبحث اول: پیشینه تاریخی جرائم رایانه‌ای

نظر به این که بررسی پیدایش سیر تاریخی جرائم رایانه‌ای و نحوه تحول و تکامل شیوه‌های ارتکاب این نوع جرائم کمک شایانی در شناسایی ماهیت و تعریف و طبقه‌بندی آنها خواهد داشت لذا بدواً به بررسی این موضوع می‌پردازیم.جرم رایانه‌ای همانگونه که از اسمش پیداست جرمی است که مرتبط با فناوری رایانه می‌باشد.

بنا براین مروری کوتاه بر تاریخ پیدایش و تکامل رایانه در تبیین موضوع مؤثر خواهد بود. قبلاً اشاره به این نکته را لازم می‌دانم که با توجه به یکسان نبودن سطح بهره‌مندی کشورها از فناوری رایانه تاریخ پیدایش و تکامل جرائم رایانه‌ای درکشورها یکسان نیست.علی هذا ابتداً به بررسی این موضوع در کشورهای توسعه یافته می‌پردازیم سپس بطور مختصر تاریخ پیدایش رایانه وجرائم رایانه‌ای را در جمهوری اسلامی ایران مرور می‌کنیم.

الف) تاریخچه پیدا یش و توسعه رایانه

رایانه از دیر باز به شکل اولیه مطرح بوده است. در سال ۱۶۴۲ میلادی پاسکال فرانسوی ماشین حسابی را اختراع کرد که می‌توانست عملیات جمع و تفریق را انجام دهد.[۱۶] سی سال بعد این ماشین توسط یک ریاضیدان آلمانی به نام لایپ نیتز تکمیل شد این ماشین خودکار (رایانه) قادر به انجام عملیات جمع، تفریق، ضرب، تقسیم، و گرفتن ریشه‌ها بود.[۱۷] درسال ۱۸۰۱ یک فرانسوی به نام ژوزف ژاکارد کارت‌های سوراخ دار که ماشینهای نساجی را در بافتن پارچه‌های نقش دار هدایت می‌کرد، اختراع کرد. درسال ۱۸۱۲ یک فرد انگلیسی به نام چالز بابیج که اکثراً از او به نام پدر رایانه‌های نوین یاد می‌شود، نوعی ماشین حساب را به نام دستگاه تفاضلی اختراع نمود.[۱۸]بابیج به فکر ساختن وسیله‌ای که به رایانه‌های امروزی شباهت داشت افتاد ولی موفق نشد، بعد از مرگ بابیج روند توسعه رایانه تاسال ۱۹۳۷ از حرکت باز ایستاد وکارتهای منگنه شده بر دنیای پردازش داده‌ها حاکم شد. نخستین نمونه رایانه الکترونیکی بین سالهای ۱۹۳۷و ۱۹۳۸ توسط دکتر جان وینسنت آتاناسوف پرفسور فیزیک و ریاضی مطرح شد و نهایتاً منجر به ساخت رایانه ABC شد. این رایانه اولین نمونه از نسل اول رایانه‌های امروزی به شمار می‌آید.در این رایانه از لامپهای خلاء برای ذخیره‌سازی و عملیات محاسباتی و منطقی استفاده می‌شد. با استفاده از این فناوری اولین رایانه الکترو نیکی چند منظوره درسال ۱۹۴۰ در دانشگاه پنسیلوانیا برای ارتش آمریکا ساخته شد. این رایانه دارای ۳۰ تن وزن بود و فضایی در حدود یک خانه سه اتاق خوابه را اشغال می‌کرد.[۱۹]

رایانه‌های نسل اول از دهه ۱۹۴۰ میلادی برابر با دهه۱۳۲۰ شمسی وارد بازار شدند. این نوع رایانه به لحاظ تعداد کم، حجم زیاد، قیمت گران و تعداد افراد منحصر به فردی که نحوه کار با آن را می‌دانستند، دارای امنیت ذاتی بود. اگر جرمی نسبت به این رایانه‌ها یا به وسیله آنها ارتکاب یافته باشد،گزارش نشده است. رایانه‌های نسل دوم که در آنها به جای لامپ خلاء از ترانزیستور استفاده شده بود از دهه ۵۰ میلادی (برابر با ۱۳۳۰ شمسی) وارد بازار شدند، این نسل از رایانه‌های نسل اول

۱۶–پرهامی، بهروز،آشنایی با کامپیوتر، انتشارات علم وصنعت تهران،۱۳۷۱،ص۱۸۵

۱۷– انزالی، امیر اسعد،کامپیوترهای امروزی، مجتمع فنی تهران، چ دوم،۱۳۷۴،ص۲

۱۸– پرهامی، همان

۱۹– پاکزاد، بتول، جرائم کامپیوتری، پایان نامه کارشناسی ارشد، دانشگاه شهید بهشتی، ۱۳۷۵، ص۹

کوچکتر، ارزانتر و سریعتر بودند. در این دهه انواع مشاغل و علوم شیفته استفاده از رایانه شدند. بـه لحـاظ گرانـی و تعـداد کـم رایانه‌ها از آنها به صورت تقسیم تجاری زمان استفاده می‌شد، به این نحو که مالکین رایانه‌ها زمان استفاده از آنهـا را بـه تجـار، مدارس،کتابخانه‌ها و برنامه نویسانی که خود قادر به خرید رایانه نبودند اجاره می‌دادند.

رایانه‌های نسل دوم برخلاف نسل اول مستقل نبودند زیرا به دلیل کثرت افراد و مشاغلی که از یک رایانه اسـتفاده مـی‌کردنـد داده‌ها و برنامه‌های ذخیره شده آنها در دسترس دیگران قرار می‌گرفت و آسیب پذیر بودند. بدین ترتیب اولین دروازه‌های هـک کردن گشوده شدند و با وجود تلاش مدیران سیستم‌ها و فروشندگان محصولات امنیتی رایانه‌ای و مجریان قانون، آن دروازه‌هـا هیچگاه بسته نشدند.

نسل سوم رایانه‌ها که به جای ترانزیستور از آی.سی(IC) در ساخت آن استفاده شده بود از اوایل دهه ۱۹۶۰ مـیلادی برابـر بـا دهه ۱۳۴۰ شمسی وارد بازار شد این رایانه‌ها دارای حجم و قیمت کمتر و قدرت پردازش و ذخیره بیشتری نسبت به نسـل‌هـای قبل بودند، ولی باز هم در رده رایانه‌های بزرگ محسوب می‌شدند. این رایانه‌ها برای سازمان‌های بزرگ مناسب بودند، ولی برای مؤسسات کوچکتر به لحاظ کاربردهای ویژه و قیمت زیاد خرید و هزینه نگهداری مناسب و مقرون به صرفه نبودند.

رایانه‌های شخصی (PC) که نسل چهارم محسوب می‌شوند از اوایل دهه ۱۹۷۰ میلادی وارد بازار شـدند. از خصوصـیات ویـژه رایانه‌های نسل چهارم به کارگیری مدارهای مجتمع الکترونیکی در تراکم زیاد بود که باعث کاهش فوق‌العاده حجـم و افـزایش قدرت و پردازش آنها گردید.

رایانه‌های شخصی اولیه فاقد برنامه بودند. لذا خریدار باید برای راه‌اندازی آنها، برنامه مورد نیاز خـود را در آن مـی‌نوشـت. ایـن رایانه‌ها برای مالک خود این فرصت را فراهم می‌کرد که در هنگام فرا گرفتن برنامه‌نویسی با هک کردن نیز آشنا شود. از دیگـر خصوصیات رایانه‌های نسل چهارم استفاده از حافظه نیمه‌هادی، ریز پردازنده، سیستم‌های محاوره‌ای، پردازش، ارتبـاط مسـتقیم وشبکه‌های رایانه‌ای بوده است. [۲۰]

رایانه‌های شخصی توانایی محاسبه قدرتمندتر را برای افرادی که مشتاقانه در پی یافتن روش‌هایی برای بهره‌بـرداری از قابلیـت سیستم‌ها بودند ایجاد نمودند. اما این شبکه‌های رایانه‌ها بودند که در واقع دریچه‌های سد شده در برابر هک کردن را برای همه هک‌های بعدی باز کردند.

اگر چه فشردگی مدارهای الکترونیک در رایانه‌های نسل چهارم باعث کاهش فوق‌العاده حجم آنها گردید و این قابلیـت سـاخت ریز رایانه‌ها و نتیجتاً رایانه‌های شخصی را امکان پذیر ساخته است، اما این قابلیت مانع از ساخت رایانه‌های بزرگ نشده است.

رایانه‌های نسل چهارم و بعد از آن از جهت حجم و قدرت کارائی به چهار دسته تقسیم شده‌اند:

۱– ابر رایانه‌ها که تعداد آنها اندک است و در فضا نوردی و پروژه‌های عظیم علمی از آنها استفاده می‌شود

۲–رایانه‌های بزرگ که کارهای یک وزارتخانه یا مؤسسهٔ عظیم را انجام می‌دهند.

۳–رایانه‌های کوچک که مقداری از رایانه‌های بزرگ کوچکتر هستند.

۴–ریز رایانه‌ها که کم قدرت هستند. رایانه‌های شخصی جزء این دسته محسوب می‌شوند بعلاوه در ساخت دستگاه‌های کوچک مثل سیستم احتراق اتومبیل و غیره از آنها استفاده می‌شود. [۲۱]

۲۰– پاکزاد همان،ص۱۰

۲۱–انزالی، همان.۴۰–۳۷

شبکه‌های رایانه‌ای

با عنایت به اینکه شبکه‌های رایانه‌ای بعد از ساخته شدن رایانه‌های نسل چهارم که قابلیت ارتباط با رایانه‌های دیگر را داشتند به وجود آمدند و استفاده از فناوری شبکه‌های رایانه‌ای و ارتباط بین شبکه‌ای موجب انقلابی بزرگ در فناوری اطلاعات و ارتباطات گردید لذا در اینجا اشاره‌ای مختصر به شبکه‌های رایانه‌ای خواهیم داشت.

شبکه‌های رایانه‌ای مجموعه‌ای از رایانه‌های متصل به یکدیگرندکه بتوانند بین یکدیگر اطلاعات مبادله کنند. امروزه این اتصال ممکن است به وسیله سیم، لیزر، مایکروویو یا ماهواره مخابراتی انجام گیرد. شبکه‌های رایانه‌ای در بدو امر ابزاری مرموز بودند که صرفاً که به وسیله متخصصانی معدود به کار گرفته می‌شدند. هر سازنده سیستم‌های رایانه‌ای برای شبکه‌اش معماری خاص خود را داشت. و هیچیک از این معماری‌ها با همدیگر سازش نداشت ولی امروزه وضعیت با گذشته به کلی متفاوت است. تقریبًا کلیه دست‌اندرکاران صنایع مرتبط با رایانه روی مجموعه‌ای از استانداردهای بین‌المللی به توافق رسیده‌اند. اکثر رایانه‌ها از رایانه‌های شخصی گرفته تا ابر رایانه‌ها می‌توانند اجزایی از شبکه‌ها باشند. شبکه‌های رایانه‌ای بر حسب فاصله فیزیکی به شبکه‌های محلی و شبکه‌های راه دور تقسیم می‌شوند. شبکه‌های محلی معمولاً ارتباط بین چند رایانه واقع در یک اتاق یا یک ساختمان یا تعدادی از ساختمان‌های واقع در یک بلوک (مثل یک دانشگاه) را برقرار می‌کنند. از شبکه‌های راه دور برای ارتباط بین رایانه‌های واقع در محلهای مختلف یک شهر و یا رایانه‌های مستقر در شهرهای مختلف یک کشور استفاده می‌شود.[۲۲]

باتوجه به اینکه هر یک ازشبکه‌ها اجزاء مستقلی هستند که نیازهای یک گروه خاص را برآورده می‌کنند، برای ارتباط بین شبکه‌های مختلف واقع در یک شهر یا یک کشور یا دو یا چند شهر یا کشور یا قارهٔ مختلف از فناوری ارتباط بین شبکه‌ای (Internet working)استفاده می‌شود.[۲۳]

اینترنت یک سرویس بین شبکه‌ای بین‌المللی است که میلیونها شبکه رایانه‌ای را با کاربرهای متفاوت به هم مرتبط نموده است. پیش نمونه اینترنت با عنوان آرپانت توسط وزارت دفاع آمریکا درسال ۱۹۶۹ ایجاد شد. آرپانت ابتدا صرفاً به وزارت دفاع آمریکا تعلق داشت. درسال ۱۹۷۱ گسترش بانکها، دانشگاه‌ها و آژانس‌های دولتی را دربرگرفت. درسال ۱۹۷۳ کشورهای دیگر به آن متصل شدند و در ۱۹۸۶ افراد عادی نیز امکان دسترسی به آن را پیدا کردند. درسال ۱۹۸۹ آرپا مدیریت آرپانت را متوقف کرد زیرا آرپانت براثر مجتمع شدن با شبکه‌های دیگر تبدیل به اینترنت شده بود. شبکه جهان گستر که همهٔ ما هر روز مطالبی در باره آن می‌شنویم از سوئد نشأت گرفت.[۲۴]

امروزه میلیونها نفر از طریق سرویس‌های مختلف اینترنت شامل ایمیل (پست الکترونیک)، وب سایت، وبلاگ،چت، تابلوهای اعلانات، گروههای خبری و غیره به تبادل اطلاعات می‌پردازند.

رایانه‌های نسل پنجم از نظر حجم تفاوتی بارایانه‌های نسل چهارم ندارند از ویژگی‌های این نسل هوشمند بودن آنها است این رایانه‌ها مجهز به هوش مصنوعی هستند. یعنی رایانه می‌تواند فکر کند. میزان وگسترهٔ فکر رایانه بستگی به برنامه‌ای دارد که به آن داده باشند.

۲۲- آندرواس، تانن بام، شبکه‌های کامپیوتری، ترجمه دکتر محمد قدسی، شورای عالی انفورماتیک،چ دوم،۱۳۷۶،ص۲و۴

۲۳- داگلاس‌ای، کامر، ارتباط بین شبکه‌ای، ترجمه وحید فراهانی‌زاده شورای عالی انفورماتیک،۱۳۷۵،ص۱

۲۴- جینادی، آنجلیز، همان

رایانه‌های نسل ششم رایانه‌هایی خواهند بود که مدارهای داخلی‌شان کپی‌برداری از مغز انسان است به نحوی که بتوان رایانه را به انجام کارهایی نظیر مغز انسان کرد.[۲۵] در رایانه‌های نسل آینده از فناوری نانو استفاده خواهد شد و نانو رایانه‌ها و نانو روبات‌ها[۲۶] در بسیاری از علوم انقلابی جدید ایجاد خواهند کرد.

«یکی از تحولات مبتنی بر فناوری نانو که به تازگی بسیار مورد توجه قرار گرفته فناوری حافظه میلی پید (به معنای هزار پا) متعلق به شرکت آی. بی. ام است با این فناوری می‌توان به گنجایش حافظه‌ای تا حدود یک تریلیون بیت در هر اینچ مربع دست یافت. یکی از برندگان جایزه نوبل که با ای. بی. ام همکاری می‌کند گفته است:

رهیافت نانو مکانیکی امکان افزایش ذخیره‌سازی داده‌ها را تا هزار برابر کنونی فراهم خواهد ساخت. با گامهای نخستی که درفناوری نانو برداشته شده می‌توان امکان ساخت پردازنده‌ای به اندازهٔ بیست نانو متر [یعنی یک ده هزارم یک تار موی انسان] فراهم آورد. البته عده‌ای معتقدند که این تحولات به این زودی‌ها مورد نیاز نخواهد بود.[۲۷]

ب) تاریخ پیدایش و تحول جرم رایانه‌ای

با توجه به اینکه ابعاد منفی پدیده‌ای که به منظور خدمت به انسان خلق شده است، لزوماً همزمان با آن بروز نمی‌کنند، بنابراین به طور قطع جرم رایانه‌ای مدت زمانی بعد از اختراع و به کارگیری رایانه واقع شده است. گفته شده است که اولین جرم رایانه‌ای در سال ۱۸۰۱ ارتکاب یافته است بدین صورت که بعد از این که ژوزف ژاکارد فرانسوی کارت خودکارسازی بافندگی را اختراع کرده و به کار گرفت، کارگران تحت امر وی که نگران از دست دادن شغل خود بودند دست به اقدامات خرابکارانه علیه رایانه مذ کور زدند.[۲۸] واقعیت این است که آنچه اکثرحقوقدانان تحت عنوان پدیده جرم رایانه‌ای از آن نام می‌برند، نوع خاصی از سوء استفاده‌ها است. که بعد از اختراع و به کارگیری نسلهای مختلف رایانه‌های جدید از این وسیله به عمل آمد ویا علیه آن به وقوع پیوسته است، بنابراین اولین جرم رایانه‌ای بعد از بکارگیری نسل اول رایانه‌های امروزی بوقوع پیوسته است.

کسانی که در زمینه تاریخچه پیدایش جرائم رایانه‌ای پژوهش‌هایی را انجام داده‌اند گفته‌اند که واژه جرم رایانه‌ای برای اولین بار در مطبوعات عمومی و در ادبیات علمی دههٔ ۱۹۶۰ میلادی ظاهر شد. این بدان معنی نیست که در دهه‌های ۱۹۴۰ و۱۹۵۰ که در رایانه‌های نسل اول و دوم مورد استفاده قرار گرفته‌اند، جرمی به وسیله این رایانه‌ها یا علیه آنها واقع نشده باشد. چه بسا جرائمی در این مدت در این خصوص ارتکاب یافته باشد، لیکن به دلایل مختلف مانند عدم اطلاع بزهکاران و یا عدم آشنایی مأمورین کشف جرم با رایانه کشف نشده باشد و یا حتی اگر کشف شده و مورد رسیدگی هم قرار گرفته باشد به لحاظ جزئی بودن موضوع جرم اعلام نشده باشد و یا به لحاظ عدم آشنایی حقوقدانان و سایر دست اندرکاران با اصطلاح جرم رایانه‌ای ارتکاب جرمی تحت این عنوان گزارش نشده باشد و شاید به لحاظ قلت تعداد وچشمگیر نبودن، این گونه جرائم در دهه‌های ۱۹۴۰و ۱۹۵۰ مورد توجه قرار نگرفته‌اند.

۲۵- انزالی، همان،ص۷۸

۲۶- فناوری نانو در ساده ترین شکل آن بیانگر آمایش مواد در سطح اتم یا مولکول است. نام آن از واژه نانومتر گرفته شده است که یک واحد اندازه‌گیری علمی و بیانگر یک میلیاردم متر است. ضخامت موی انسان بین۱۰۰ تا ۲۰۰ هزار نانو متر است. نانو روباتها وسایل میکروسکوپی هستند که قادرند وظایف معینی را در سطح اتم یا زیر اتم انجام دهند.

۲۷- خبرنامه انفورماتیک، مقاله فناوری کاربردی نانو، ترجمه محمد خیام روحانی، شورای عالی انفور ماتیک، دی ماه ۱۳۸۱ ش۸۵، ص۴۳

۲۸ – دزیانی محمد حس،ابعاد جزایی کاربرد کامپیوتر و جرائم کامپیوتری،خبرنامه انفورماتیک، اسفند ۷۳،ص۱۵۳

تحقیقات انجام شده نشان می‌دهد که جرم رایانه‌ای به تدریج شروع شده اما در یک روند افزایشی تـوأم باسـرعت ادامـه یافتـه است. تا دهه ۱۹۷۰ میلادی تعداد سوء استفاده‌های رایانه‌ای در کشورهای توسعه یافته به قدری کم بوده است که این کشـورها ترجیح می‌دادند در چارچوب قوانین سنتی با این جرائم برخورد کنند.

بررسی قوانین مربوط به جرائم رایانه‌ای و رویه قضایی کشورهای توسعه یافته بیانگر این است که این کشـورها در دهـهٔ ۱۹۷۰ بدواً نسبت به جرائم رایانه‌ای علیه محرمانگی (جرائم علیه حقوق فردی) عکس‌العمل نشان داده‌اند و بعد از آن شروع به تغییر و اصلاح قوانین مربوط به جرائم اقتصادی و سپس جرائم علیه مالکیت معنوی کرده‌اند. ترتیب عکس‌العمل قانونی کشورها نسـبت به انواع جرائم رایانه‌ای ممکن است ناظر بر ترتیب پیدایش این جرائم باشد و ممکن است ناظر به عدم مقاومت بعضی از قوانین نسبت به قوانین دیگر در برابر جرائم رایانه‌ای باشد.

رشد فزاینده جرائم رایانه‌ای پس از به وجود آمدن رایانه‌های شخصی و شبکه‌هـای رایانـه‌ای مخصوصـاً شـبکه‌هـای رایانـه‌ای بین‌المللی مانند اینترنت نه تنها موجب افزایش جرائم علیه محرمانگی، جرائم اقتصادی و جرائم علیه مالکیـت فکـری از طریـق سیستم‌های رایانه‌ای گردید، بلکه قابلیت تعرض به دیگر اهداف و منافع مورد حمایت یک قانون را به وجود آوردند جرائمی مانند تولید، عرضه، توزیع و نگهداری انواع پورنوگرافی (هرزه‌گری) و مفاد نژادپرستانه از طریق سیستم‌ها وشبکه‌های رایانه‌ای از جمله این جرائم هستند.

واژه‌هایی مانند جرم فناوری اطلاعات و جرم سایبر و جرم اینترنتی بعد از فراهم آمـدن امکـان اسـتفاده عمـوم از اینترنـت وارد ادبیات حقوق کیفری اطلاعات گردید.

یکی از محققین و اساتید برجسته حقوق که بیشترین کتابها و مقالات را نسبت به سایر محققـین در خصـوص حقـوق کیفـری اطلاعات وجرم رایانه‌ای به رشته تحریر درآورده است در کتاب "پیدایش بین‌المللی حقوق اطلاعات کیفری"می‌گوید:

«اولین کیس‌هایی که جرم رایانه‌ای نامیده شده ابتدائا در مطبوعات عمومی و در ادبیات علمی دهه ۱۹۶۰ ظاهر شد این کیس‌ها شامل سوء استفاده‌های ابتدایی از رایانه، سابو تـاژ (خرابکـاری) رایانـه‌ای، جاسوسـی رایانـه‌ای و اسـتفاده‌هـای غیـر قـانونی از سیستم‌های رایانه‌ای بود.

چون اکثر گزارشات بر مبنای نوشته‌های روزنامه‌ها بود در مورد واقعیت یا خیالی بودن پدیده جدید جرم رایانه‌ای بحـث و تردیـد وجود داشت. از اواسط دهه ۱۹۷۰ مطالعات تجربی در مورد جرم رایانه‌ای با استفاده از متدهای تحقیقـاتی رشـته جـرم شناسـی انجام شد. این مطالعات ناظر به برخی از جرائم رایانه‌ای می‌شد. اما در همان حال تعداد زیـادی مـوارد، غیـر مکشـوف مانـده و خطرات زیادی نیز در بطن خود داشت.

در دهه ۱۹۸۰ نظرات علمی و عمومی در مورد جرم رایانه‌ای به سرعت تغییر یافت و مشخص شد که جرم رایانه‌ای محـدود بـه جرائم اقتصادی نبوده همه تعرضات نسبت به همه منافعی را شامل می‌شد و مثلاً سوء استفاده از رایانه بیمارسـتان یـا تخلفـات رایانه‌ای نسبت به حقوق خصوصی و فردی که جنبه اقتصادی ندارند و اساساً این موارد را جدا از جرم رایانه‌ای بررسی کرده‌انـد. موج وسیعی از سرقت برنامه‌ها سوء استفاده‌ها از صندوقهای پرداخت و استفاده از مخابرات موجب شد انعطاف جامعه اطلاعـاتی برانگیخته شده نیاز برای استراتژی جدید امنیت داده پردازی و کنترل جرم احساس شود.»[۲۹]

۲۹- زیبر، اولریش، پیدایش بین‌المللی حقوق کیفری اطلاعات ترجمه محمد حسن دزیانی، جزوه حقوق کامپیوتر،ج۳،شورای عالی انفور ماتیک

« در حال حاضر بیشتر نظرها در زمینه جرائم رایانه‌ای به انتقال غیر قانونی سرمایه‌ها با استفاده از ابزار الکترونیکی، خرابکاری، ویروس‌ها، کرم‌های رایانه‌ای و همچنین جعل اسناد با استفاده از رایانه معطوف است. خطر خرابکاری مخصوصاً در سال ۱۹۸۹ آشکار شد. زمانی که دادرسی‌های کیفری در جمهوری فدرال آلمان معلوم کرد که خرابکارانی با استفاده از شبکه‌های اطلاعاتی بین‌المللی به اطلاعاتی در آمریکا و انگلستان و دیگر کشورهای خارجی دست یافته‌اند و حاصل کار خود را به کشور شوروی سابق فروخته‌اند. تقریباً در همان زمان (۱۹۸۸) خطر ویروس‌ها وکرم‌ها هم معلوم شد. زمانی که (Internet- worm) توسط یک دانشجوی آمریکایی ساخته شده بود، در طی چند روز نزدیک به ۶۰۰۰ سیستم رایانه‌ای را در اینترنت مختل کرد. بعد شکلهای جدید بزهکاری در زمینه تکنیک‌های ارتباط سمعی بصری (مثلاً در زمینه سیستم مینیتل فرانسه و یا قسمت‌های ارتباط ماهواره‌ای) ادامه جرائم اطلاعات را افزایش دادند»[۳۰]

زیبز در مقاله "جرم رایانه‌ای و حقوق اطلاعات کیفری"خود که متن سخنرانی وی در اداره بازرسی و مدیریت رایانه وزارت امنیت عمومی جمهوری خلق چین در سپتامبر (۱۹۹۵) است،

می‌گوید:

«بحث درباره مبدأ سوء استفاده رایانه‌ای در بیشتر کشورها از دهه (۱۹۶۰) با به خطر افتادن حقوق فردی شروع شد که تحت عنوان حمایت از داده‌ها مورد بحث قرار گرفت و بدواً به نظر نمی‌رسید که بحثی از مباحث مربوط به جرم رایانه‌ای باشد.در این دهه با سیطره رایانه‌ها و در بسیاری از کشورهای غربی این امر به واقعیت پیوست که، جمع‌آوری، ذخیره‌سازی، انتقال و مرتبط‌سازی داده‌های شخصی حقوق مربوط به شخصیت شهروندان را به خطر می‌اندازد.

تجاوزات آشکار به حقوق فردی و خصوصی در زمینه اسرار شغلی حمایت شده مرسوم (به وسیله حقوق جزا) به ویژه مسائل مربوط به اسرار رسمی بعلاوه شرط محرمانگی امری شناخته شده برای پزشکان، حقوقدانان، بانکها و مأمورین محسوب می‌شود. ازدهه۱۹۷۰مباحثات در مورد سوء استفاده رایانه‌ای نه تنها به وسیله جرائم مربوط به حمایت از داده‌ها بلکه جرائم اقتصادی مرتبط با رایانه را در برگرفته است که امروز به عنوان محور و حوزه اصلی جرم رایانه‌ای مورد توجه قرار می‌گیرند. و بدواً به طور انحصاری به وسیله این عبارات مشخص می‌شوند. در این زمینه جرائم اصلی عبارتند از: سوء استفاده رایانه‌ای، سابوتاژ رایانه‌ای، اخاذی رایانه‌ای، نفوذ یافتن، جاسوسی، سرقت نرم افزار و دیگر اشکال سرقت محصولات.»[۳۱]

مترجم فارسی مقاله جرم رایانه‌ای و حقوق کیفری اطلاعات، این قسمت از مقاله را نقد کرده و می‌گوید:

«نکته‌ای که پرفسور زیبر به آن اشاره کرده و شروع بحث سوء استفاده‌های رایانه‌ای را در آن متمرکز کرده است شاید تا حدی بحث برانگیز باشد. بی شک دهه ۱۹۶۰ نقطه آغاز جرائم رایانه‌ای است اما این که شروع بحث از حیص موضوعی با جرائم اقتصادی مرتبط بارایانه بوده است یا با جرائم علیه شخصیت معنوی وحریم خصوصی افراد، (یعنی آنچه درحقوق اساسی بدان حقوق فردی گویند) متنازع فیه است. زیرا قضیه شناخته شده‌ای که معمولاً به عنوان اولین جرم رایانه‌ای کشف شده مطرح می‌شود، قضیه الدن موریس است. در این قضیه موریس وجوه مربوط به شرکت یا به عبارت بهتر مشتریان را به خود اختصاص

۳۰- زیبر،الریش، جرائم کامپیوتری و دیگر جرائم مرتبط با فناوری اطلاعات، ترجمه محمد حسن دزیانی، جرائم کامپیوتری ج۴، شورای عالی انفورماتیک،ص۵

۳۱- زیبر، اولریش، جرم کامپیوتری و حقوق کیفری اطلاعات، ترجمه م دزیانی، جزوه جرائم کامپیوتری،ج۴،دبرخانه شورلی عالی انفور ماتیک،۱۳۷۶، ص۱۱۵و۱۱۶

داد. یا قضایایی همچون شرکت بیمه اکویتی فاندینگ، ولو، ژرمن هرشتات و...همه ناظر بر جرائم اقتصادی یا به عبارت دیگر جرائم علیه اموال است. به هر حال خواننده در این مورد با رأی از پرفسور زیبر برخورد می‌کند که از حیث تاریخی نیازمند بحث‌های فراوان است.»[۳۲]

شاید آنچه باعث شده است که ناقد برخلاف پرفسور زیبر به این نتیجه برسد که بحث در مورد جرایم رایانه‌ای مربوط به حمایت از داده‌ها و حقوق فردی متأخر بر بحث مربوط به جرائم رایانه‌ای اقتصادی بوده است، عدم توجه به نکته ظریفی باشد که دکتر زیبر به آن اشاره کرده است. آن نکته این است: «بدواً به نظر نمی‌رسیده که جرائم علیه حقوق فردی که به وسیله رایانه ارتکاب می‌یابند بخشی از مباحث مربوط به جرم رایانه‌ای باشند.» لذا علی‌رغم این که بحث در مورد جرائم علیه داده در مجامع علمی مطرح بوده است، مطبوعات عمومی به آن نپرداخته‌اند. در نتیجه به لحاظ اهمیت و توجه بیشتر افکار عمومی به جرائم اقتصادی، جرائمی مانند قضیه «الدن موریس» و سایر قضایای مذکور به عنوان اولین جرائم مرتبط با رایانه مطرح شده‌اند.

ج) تاریخچه پیدایش حقوق کیفری اطلاعات

اول: واکنش تقنینی کشورها در مورد جرائم رایانه‌ای

گفته شد که تا دهه ۱۹۷۰ میلادی کشورهای مختلف در چارچوب قوانین سنتی با جرائم رایانه‌ای برخورد می‌کردند. اما پیشرفت فناوری اطلاعات و تنوع و کثرت سوء استفاده‌هایی که از این فناوری به عمل آمد، حقوق جزای سنتی کشورها را به چالش کشید.

یکی از علل به چالش کشیده شدن حقوق جزای سنتی این بود که قوانین کیفری کشورها تا قبل از شیوع جرائم رایانه‌ای غالباً به حمایت از اهداف و موضوعات ملموس می‌پرداختند. با رشد فناوری رایانه، اطلاعات و داده‌های رایانه‌ای به عنوان یک موضوع غیرملموس، غیر قابل رؤیت و با ارزش، موضوع جرم رایانه‌ای قرار گرفت. حقوق جزای ماهوی که حمایت از ارزشها را بر عهده دارد در برابر تجاوز و تعدی به این ارزشها با نگرشی جدید واکنش نشان داد. این نگرش طی مراحلی موجب اصلاح سیستم‌های قضایی گردید. پرفسور زیبر آلمانی (پدر حقوق کیفری اطلاعات) به چهار مرحله از این مراحل به ترتیب زیر اشاره کرده است.

اولین مرحله اصلاح سیستم‌های قضایی غرب بود، که در حمایت از محرمانگی (حقوق خصوصی و فردی) در دهه‌های ۱۹۷۰و۱۹۸۰ ظاهر شد. این تقنین واکنشی در برابر چالش‌های جدید مربوط به حقوق خصوصی و فردی بود که به واسطه امکانات جمع‌آوری، ذخیره‌سازی و انتقال داده‌ها از طریق تکنولوژی جدید با مسائل جدید مواجه شده بود. لذا قوانین جدید حمایت از داده‌ها در حمایت از حقوق خصوصی و فردی شهروندان از جنبه اداری، مدنی و کیفری در کشورهای مختلف تصویب شد. قوانین کانادا و استرالیا در ۱۹۷۲، سوئد ۱۹۷۳، آمریکا ۱۹۷۴، آلمان۱۹۷۷، فرانسه، نروژ، اتریش و دانمارک ۱۹۸۸، ایسلند ۱۹۸۱، بریتانیا ۱۹۸۴، ایرلند، ژاپن و هلند ۱۹۸۸ تصویب شده‌اند و بعضاً این قوانین جدید مورد اصلاح قرار گرفته‌اند.

مرحله دوم از موج قوانین اصلاحی ناظر بر جرائم اقتصادی مرتبط با رایانه در اواخر دهه۱۹۷۰و دهه ۱۹۸۰است. آمریکا درسال ۱۹۷۶ (در سطح ایالات)، ایتالیا ۱۹۷۸، استرالیا ۱۹۷۹، بریتانیا۱۹۸۱، آمریکا۱۹۸۴(درسطح فدرال)،دانمارک وکانادا

۳۲- دزیانی محمد حسن، جزوه جرائم کامپیوتری،ج۲،۱۳۷۶،ص۱۴

۱۹۸۵،آلمان۱۹۸۶، سوئد و شیلی۱۹۸۷، اتریش، ژاپن و نروژ ۱۹۸۷، فرانسه و یونان ۱۹۸۸، فنلاند و بریتانیا ۱۹۹۰ قوانینی در خصوص جرائم رایانه‌ای اقتصادی وضع کرده‌اند که بعضی از این قوانین چند بار اصلاح شده‌اند.

مرحله سوم قوانین اصلاحی در دهه۱۹۸۰ ناظر بر جرائم مالکیت معنوی مرتبط با رایانه است. بعد از این که برنامه‌های رایانه‌ای در دهه ۱۹۷۰ تحت حمایت حق اختراع قرار گرفت،قوانین اصلاحی برنامه های رایانه‌ایرا مشمول کپی رایت (مالکیت معنوی)قرار دادند. کشور آمریکا در ۱۹۸۰، مجارستان ۱۹۸۳، استرالیا، هند و مکزیک ۱۹۸۴، شیلی، آلمان، فرانسه، ژاپن و انگلستان در ۱۹۸۵ برزیل، کانادا و اسپانیا در ۱۹۸۸، دانمارک، کلمبیا و سوئد۱۹۹۰ و نروژ در ۱۹۹۱ قوانین مربوط به مالکیت معنوی (کپی رایت) خود را اصلاح کرده‌اند. و پیشرفت‌های کلی در زمینه حمایت جزایی از مالکیت معنوی نیز حاصل شده است.

مرحله چهارم اصلاحات بین‌المللی قوانین در مورد قوانین آئین‌دادرسی است.[۳۳] بسیاری از کشورها مانند آمریکا، کانادا، آلمان و دیگر کشورهای اروپایی قوانینی را در خصوص تفتیش و توقیف داده‌های رایانه‌ای وضع کرده‌اند.«در این خصوص می‌توان به تدوین قوانین انگلیس ۱۹۸۴،دانمارک ۱۹۸۵،آمریکا ۱۹۸۶ وهلند ۱۹۹۴ اشاره نمود.»[۳۴]

مرحله پنجم اصلاح قوانین در مورد جرائم مربوط به محتوا است. به عنوان مثال بسیاری از کشورها قوانینی وضع کردند که تهیه، توزیع، عرضه و نگهداری پورنوگرافی(هرزه نگاری) کودکان از طریق سیستم‌ها وشبکه‌های رایانه‌ای را جرم تلقی کرده است.

در سال۲۰۰۰ مؤسسه بین‌المللی مک کانل مطالعه‌ای در مورد وضعیت قوانین وضع شده در ارتباط با جرائم رایانه‌ای در چهار گوشه جهان به عمل آورده است. این مؤسسه از کشورها خواسته است که چنانچه قوانین و یا پیش‌نویس قوانینی در این خصوص دارند ارسال کنند، در غیر این صورت اعلام نمایندکه هیچ اقدام مثبتی انجام نداده‌اند.

کشورهایی که قوانین خود را ارائه کرده‌اند به گونه‌ای مورد ارزیابی قرار گرفته‌اند که مشخص شود آیا قوانین جزایی آنها فضای شبکه‌های رایانه‌ای را شامل می‌شود یا نه؟ و آیا ده نوع جرم رایانه‌ای را که در قالب چهار دسته کلی به شرح زیرطبقه بندی شده‌اند پوشش می‌دهد یا نه؟ ده نوع جرم مورد سوال عبارتند از:

۱- جرائم داده شامل شنود الکتریکی داده، تغییر داده وسرقت داده

۲- جرائم شبکه از قبیل اختلال در شبکه وخرابکاری در شبکه

۳- جرائم دسترسی به اطلاعات شامل نفوذ یافتگی و انتشار ویروس

۴- جرائم مرتبط شامل کلاهبرداری وجعل رایانه‌ای ومعاونت عاملان جرائم رایانه‌ای

سی و سه کشور (از بین بیش از ۵۰ کشور) مورد بررسی تا آن تاریخ نسبت به روز آمد کردن قوانین خود به منظور برخورد با انواع جرائم رایانه‌ای هیچ اقدامی انجام نداده بودند ولی اکثراً در حال تهیه پیش‌نویس قوانین بودند. این کشورها عبارتند از:

ایران، آلبانی، بلغارستان، بورندی، کوبا، دومینیکن، مصر، اتیوپی، فیجی، گامبیا، مجارستان، اردن، نیکاراگوئه، قزاقستان، لیتونی، لبنان، لسوتر، مالت، مولداوی، مراکش، زلاندنو، نیجریه، رومانی، آفریقای جنوبی، ویتنام، یوگسلاوی،زامبیا، زیمبابوه

۳۳- زیبر،اولریش،پیدایش بین المللی حقوق کیفری اطلاعات،ترجمه،دزیانی،جرائم کامپیوتری،ج۳،دبیرخانه شورای عالی انفورماتیک،۱۳۷۶،ص۲۰

۳۴- باستانی،برومند، جرائم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری، رساله مقطع کارشناسی ارشد، دانشگاه آزاد اسلامی واحد مرکز ۱۳۸۱ ص۱۰۵

ده کشور از کشورهای مورد بررسی برای برخورد با حداکثر پنج نوع از ده نوع جرم رایانه‌ای فوق‌الذکر قانون وضع کرده‌اند که عبارتند از: ۱- برزیل ۲- کانادا ۳- شیلی ۴- چین ۵- چک ۶- دانمارک ۷- مالزی ۸- لهستان ۹- اسپانیا ۱۰- فرانسه
۹ کشور نیز برای برخورد با بیش از شش نوع از انواع جرم رایانه‌ای فوق‌الذکر قانون وضع کرده‌اند که عبارتند از: ۱- آمریکا ۲- انگلیس ۳- ترکیه ۴- پرو ۵- ژاپن ۶- موریس ۷-استونی ۸- استرالیا ۹-هند
کشور فیلیپین برای هر ده نوع جرم رایانه‌ایمذکور قانون وضع کرده است.[۳۵]

دوم: فعا لیت سازمانهای بین‌المللی در خصوص جرائم رایانه‌ای

انسجام سیستم‌های رایانه‌ای و ارتباط راه دور، بویژه وجود پدیده‌ای به نام اینترنت محدودیتهای جغرافیایی و مرزهای ملی را برای ارتکاب جرائم رایانه‌ای از بین برده است. مرزهای ملی که قبلاً موانع ارتکاب جرم محسوب می‌شدند امروزه معنای خود را از دست داده‌اند. مجرمین می‌توانند بدون توجه به مکان فیزیکی که در آن قرار دارند، در هر نقطه دنیا که بخواهند مرتکب جرم شوند و بدون توجه به بعد مکان، در یک زمان، در ارتکاب یک جرم، با مجرمین مستقر در کشورهای مختلف مشارکت داشته باشند. بنابراین به لحاظ خصیصه فراملی جرائم رایانه‌ای، اقدامات بین‌المللی فراوانی برای دستیابی به سیاست جنایی بین‌المللی ناظر بر این جرائم انجام شده است. فعالیت‌های بین‌المللی برای مبارزه با جرائم رایانه‌ای از دهه ۱۹۸۰ شروع شد. سازمان‌هایی مانند سازمان همکاری وتوسعه اقتصادی، انجمن بین‌المللی حقوق جزا، سازمان ملل متحد، اینترپول، شورای اروپا و مجمع کشورهای شرکت‌کننده درکنفرانس بین‌المللی مبارزه با جرائم سایبر (۲۰۰۱) بوداپست اقدامات ارزنده‌ای را در این خصوص انجام داده‌اند.

۱- سازمان همکاری وتوسعه اقتصادی(OECD)

اولین کوشش بین‌المللی در مورد بحث و بررسی مشکلات حقوق جزا در برابر جرم رایانه‌ای توسط سازمان همکاری و توسعه اقتصادی (OECD) صورت پذیرفت. این سازمان در سال ۱۹۷۷ شروع به اتخاذ رهنمودهایی ناظر به حمایت از حقوق فردی و جریان فراملی داده‌های شخصی کرد. کمیته تخصصی این سازمان کار خود را در زمینه ایجاد هماهنگی بین‌المللی بین قوانین کیفری برای مبارزه با جرائم اقتصادی رایانه‌ای را شروع کرد و در سال ۱۹۸۹ لیستی از سوء استفاده‌های رایانه‌ای را ارائه داد. در سال ۱۹۸۹ این سازمان کارش را در خصوص امنیت سیستم‌های رایانه‌ای ادامه داد.

۲- سازمان ملل متحد

در هفتمین کنگره سازمان ملل متحد درسال ۱۹۸۵ "جرم رایانه‌ای" از جمله موارد مطروحه در گزارش دبیر کل این سازمان بود. به عنوان برنامه تدارکاتی هشتمین کنگره سازمان ملل متحد اجلاس مقدماتی منطقه‌ای آسیا و اقیانوس آرام نگرانی خود را درباره آثار پیشرفت‌های تکنولوژی و انعکاس آن در جرائم رایانه‌ای اعلام داشت. در اجلاس مقدماتی منطقه‌ای اروپا پیشنهاد شد که مبارزه بین‌المللی با جرائم رایانه‌ای از سوی هشتمین کنگره سازمان ملل متحد و کنگره‌های پس از آن مورد حمایت و توجه قرار گیرد. در دوازدهمین اجلاس عمومی کنگره هشتم که در ۱۹۹۰ برگزار شد، نماینده کانادا پیش‌نویس قطعنامه‌ای را در مورد جرائم رایانه‌ای تسلیم کنگره کرد. در سیزدهمین اجلاس عمومی کنگره هشتم، قطعنامه مذکور پذیرفته شد. در این قطعنامه از کشورهای عضو خواسته شده است که به تلاشهای خود در زمینه مبارزه با جرائم رایانه‌ای از طریق مدرنیزه کردن قوانین و

۳۵- روحانی، محمد خیام، ترجمه مقاله جرائم کامپیوتری و ...مجازات، خبرنامه انفورماتیک، ش۷۷، فروردین ۱۳۸۰،ص۳۸،۳۷،۳۶

دادرسی های ملی، ارتقاء ضوابط پیشگیرانه و امنیتی رایانه، اتخاذ تدابیری برای ایجاد حساسیت در مردم و قوه قضائیه برای جلوگیری از جرائم رایانه‌ای و... شدت بخشند و از دبیر کل سازمان خواسته شد تا موضوع انتشار یک نشریه فنی در مورد جلوگیری و تعقیب جرائم رایانه‌ای را مد نظر قرار دهد.

مجمع عمومی سازمان ملل متحد در قطعنامه شماره ۴۵/۱۲۱ خود اسناد و قطعنامه‌های مصوبه هشتمین کنگره را پذیرفت و از دولتها خواست تا در تبیین قوانین و دستورالعمل‌های تعیین‌کننده خط و مشی خود و بر اساس شرایط اقتصادی، اجتماعی، حقوقی، فرهنگی و سیاسی در کشور از قطعنامه‌های مزبور تبعیت کنند.[۳۶]

۳- انجمن بین‌المللی حقوق جزا (AIDP)

انجمن بین‌المللی حقوق جزا که یک سازمان غیر دولتی است در سال ۱۹۹۰ جرم رایانه‌ای را به عنوان یک موضوع مورد بحث برای اعضای خود مطرح کرد و در سال ۱۹۹۲ یک نشست مقدماتی پیرامون جرم رایانه‌ای در دانشگاه ورتسبورگ آلمان برگزار کرد و قطعنامه‌ای در مورد فهرست جرائم رایانه‌ای صادر کرد و در سال ۱۹۹۴ در نشست نهایی خود در ریودوژانیرو و در نشستهای بعدی خود مصوباتی در این خصوص داشته است.

٤- یونسکو

در اجلاس ۱۹۹۹ یونسکو در پاریس که از ۱۸ تا ۱۹ ژانویه ۱۹۹۹ باحضور خود ۳۰۰ نفر از متخصصین در حوزه مراقبت و محافظت از اطفال، متخصصین اینترنت و تهیه‌کنندگان خدمات اینترنتی و..... به منظور بررسی راههای مبارزه با سوء استفاده جنسی از اطفال، پدوفیلی (کودک دوستی به منظور سوء استفاده جنسی) و هرزه نگاری اطفال در اینترنت تشکیل شد اعلامیه مورخه۱۹۹۹/۱/۱۹ یونسکو که یک برنامه عملی برای مبارزه با جرائم اینترنتی علیه اطفال می باشد، صادر گردید.[۳۷]

۵- شورای اروپا

شورای اروپا درسال ۱۹۸۵ موضوع جرم رایانه‌ای را از طریق یک کمیته تخصصی مورد مطالعه و بررسی قرار داده است کمیته منتخب کارشناسان جرم رایانه‌ای کار خود را در ۱۹۸۵ شروع و در ۱۹۸۹ یک توصیه نامه و یک گزارش به کمیته اروپایی مسائل ناشی از جرم ارائه کرد. کمیته اخیر نیز پس از تصویب آن را به کمیته وزرای شورای اروپا فرستاد و در سپتامبر ۱۹۸۹ به عنوان یک توصیه نامه تحت عنوان R(۸۹)۹ مورد تصویب نهایی قرار گرفت. توصیه نامه دیگری در زمینه آئین‌دادرسی جرائم فناوری اطلاعات درسال ۱۹۹۵ تحت عنوان توصیه نامه۱۳(۹۵)R توسط این شورا تصویب شده است.

کمیته وزراء شورای اروپا درسال ۱۹۹۷ کمیته دیگری به نام کمیته متخصصین جرائم سایبر را تشکیل داد این کمیته پیش‌نویس کنوانسیون جرائم سایبر و گزارش توجیهی آن را در سال ۲۰۰۰ تهیه نمود.

کنوانسیون جرائم سایبر درسال ۲۰۰۱ در یک کنفرانس بین‌المللی که با شرکت کشورهای عضو شورای اروپا و چهار کشور دیگر (آمریکا، ژاپن، آفریقای جنوبی و کانادا) تشکیل گردید، به تصویب رسید وکاملترین سند بین‌المللی در مورد جرائم رایانه‌ای می‌باشد.

۳۶- جرائم کامپیوتری جلد اول، ترجمه نشریه بین‌المللی سیاست جنایی شماره‌های ۴۳و۴۴، سال۱۹۹۴، شورای عالی انفورماتیک ص۱۹و۲۰

۳۷- ر.ک حسینی بیژن جرائم اینترنتی علیه اطفال وزمینه‌های جرم‌شناسی آن پایان نامه مقطع کارشناسی ارشد، دانشگاه آزاد اسلامی واحد علوم و تحقیقات۱۳۸۲،ص۷۵

د) تاریخچه رایانه وجرائم رایانه‌ای در ایران

۱- کار برد رایانه در ایران

رایانه از اوایل سال ۱۳۴۰ یعنی در حدود ۲۲ سال پس از اختراع اولین رایانه وارد ایران شد. بانک ملی و شرکت نفت اولین نهادهایی بودند که کار با رایانه را در سال ۱۳۴۱ شروع کردند. دانشگاه تهران در سال ۱۳۴۳ کار با رایانه را شروع کرد. تعداد رایانه‌های ایران در سال ۱۳۴۵ جمعا به ۹ رایانه و در سال ۱۳۴۹ به ۷۸ دستگاه رسید. این رایانه‌ها اغلب اجاره‌ای بودند. اجاره این رایانه‌ها در سال ۱۳۴۹ برابر ۷۰۳ دلار، درسال ۱۳۵۵ معادل ۳/۵ میلیون دلار و در سال ۱۳۵۶ معادل ۴/۵ میلیون دلار بوده است. در سال ۱۳۵۶ تعداد رایانه‌های نصب شده به ۶۱۶ دستگاه رسیده بود. بعد از پیروزی انقلاب شکوهمند اسلامی ایران نهادهایی برای سیاست گذار یا امور انفور ماتیک ایجاد شد و به امور را یانه‌ای سر و سامانی بخشید. با وجود تلاشهایی که به عمل آمده و اقدامات ارزشمندی که صورت گرفته است، تا چند سال اخیر کار بری فناوری اطلاعات در کشور ما از رشد مطلوبی برخوردار نبوده است.

با سیاست‌گذاری و فعالیت نهادهای متولی فناوری اطلاعات و تلاش و سرمایه گذاری بخش خصوصی، فناوری اطلاعات در سالهای اخیر از رشد نسبتا خوبی داشته است. در حال حاضر تقریبا تمام وزارتخانه‌ها ومؤسسات دولتی مخصوصا دانشگاهها ومراکز پژوهشی و بانک‌ها برای انجام بسیاری از امور خود از سیستم‌ها و شبکه‌های رایانه‌ای استفاده می‌کنند، اما از تمام توان و کارآیی رایانه استفاده نمی‌شود. بخش خصوصی در کنار بخش دولتی و حتی با پیشی گرفتن از بخش دولتی از نیمه دوم دهه ۱۳۷۰ مبادرت به ایجاد نقاط تماس بین‌المللی (ASP) و تأسیس مراکز تهیه و ارائه خدمات اطلاع رسانی (اینترنتی) (ISP) نمودند. لذا علاوه بر مراکز دولتی و مؤسسات خصوصی بسیاری از خانواده‌های ایرانی تشویق به خرید رایانه و استفاده از سرویس‌های اینترنت شدند.کسانی که فاقد رایانه هستند از خدمات دفاتر دسترسی به اینترنت (کافی نت) استفاده می‌نمایند.

دسترسی به اینترنت در اواخر دهه ۱۳۷۰ و مخصوصاً اوایل دهه ۱۳۸۰ باعث شد که بسیاری از جوانان و کسانی که احساس می‌کردند مطلبی برای ارائه به عموم دارند از طریق ایجاد وب سایتها و وبلاگها به انتشار افکار و اندیشه‌ها و مطالب علمی، سیاسی،اقتصادی،اجتماعی، فرهنگی، مذهبی خود بپردازند.

اگر چه رایانه بیست سال بعد از اختراع وارد کشور ما گردید واز سال ۱۳۴۰ تا دهه ۱۳۷۰ (یعنی ۳۰ ساله دوم)نیز از رشد بسیار کمی نسبت به کشورهای توسعه یافته برخوار بوده است لیکن در چند سال اخیر از جهت توسعه کار بری فناوری اطلاعات رشدی بسیار سریع وفوق العاده (خصوصا در بخش خصوصی)داشته است.

حسب آماری که مسؤلین ذیربط در چند روز اخیر ارائه نموده اند،در حال حاضر حدود پنج میلیون رایانه شخصی در کشور وجود دارد. یعنی به ازای هر یکصد نفر هفت رایانه شخصی در اختیار مردم می باشد.این شاخص در جهان ۹/۲ ودر مالزی ۱۳ رایانه

است. کاربران اینترنت در ایران به ازای هر ده هزار نفر ۱۵۶ نفر می باشند.[۳۸] در جهان این شاخص ۹۷۲ نفر،در آسیا ۵۵۸ نفر، در آمریکا ۵۴۰۰ نفر و در مالزی ۲۷۳۱ نفر است.[۳۹]

۲- نهاد های متولی فناوری اطلاعات

از ورود رایانه (۱۳۴۰) تا پیروزی انقلاب شکوهمند اسلامی ایران (سال۱۳۵۷)مرکزی برای برنامه ریزی امور رایانه‌ایدر ایران وجود نداشته است.بعد از پیروزی انقلاب کمیسیون ملی انفورماتیک تشکیل گردید.لایحه قانونی شورای عالی انفورماتیک کشور در ۵۹/۴/۴ به تصویب شورای انقلاب رسید.در اجرای این لایحه درسال ۱۳۶۰ شورای عالی انفورماتیک وابسته به سازمان برنامه وبودجه به عنوان ارگان اصلی سیاست گذاری در زمینه انفورماتیک شروع به فعالیت کرد ونظارت بر مراکز رایانه‌ایکشور را برعهده گرفت. در حال حاضر بیش از پانصد وپنجاه مؤسسه وشرکت رایانه‌ایخصوصی تحت نظارت این شورا به فعالیتهای تولیدی،خدماتی

ویاتحقیقاتی در زمینه فناوری اطلاعات مشغول هستند.این شورا در اجرای قانون و آئین نامه قانون حمایت از حقوق پدید آورندگان نرم افزارهای رایانه‌ایمصوب ۱۳۷۹/۱۰/۴مبادرت به تشکیل نظام صنفی رایانه‌اینموده است.

از تاریخ ۱۳۷۷/۲/۸ شورای عالی اطلاع رسانی به منظور گسترش کاربرد فناوری اطلاعات و ارتباطات در وزارتخانه ها وسازمانهای دولتی بوجود آمد.این شورا فعالیتهای زیادی در زمینه اتوماسیون نظام اداری و گسترش کاربرد فناوری اطلاعات در زمینه های مختلفاجتماعی و اقتصادی وفرهنگی بعمل آورده است.از جمله مهمترین فعالیتهای این شورا می توان به تدوین واجرای نسبی برنامه «توسعه وکاربری فعالیت ارتباطات واطلاعات ایران» (تکفا) اشاره کرد.

به موجب قانون وظایف و اختیارات و تغییر نام وزارت پست وتلگراف وتلفن مصوب سال ۱۳۸۲سیاست گذاری وتوسعه فناوری اطلاعات به شورای عالی فناوری اطلاعات واگذار گردیده است.رئیس شورا به پیشنهاد وزیر ارتباطات و فناوری اطلاعات و با موافقت رئیس جمهور منصوب می‌شود. دبیرخانه شورا در وزارت ارتباطات تشکیل می شود.

۳- جرائم رایانه‌ای و قوانین مربوطه در ایران

با توجه به این که کاربرد رایانه در ایران از ابتدای ورود آن تا دهه ۱۳۷۰ بسیار محدود بوده است،لذا جرم رایانه‌ای سابقه چندانی در کشور ما ندارد. اگر احیانا جرمی در این خصوص واقع شده باشد،گزارشی از آن منتشر نشده است. وقوع جرم رایانه‌ای به تدریج از دهه ۱۳۷۰ در ایران شروع شد.البته آمار دقیقی در این خصوص نیز دردست نمی باشد.سوء استفاده از رایانه برای ارتکاب جرائم سنتی،بکارگیری ویروس از طریق توزیع حامل های داده آلوده به ویروس،سوءاستفاده های مالی وتکثیر غیر مجاز نرم افزارهای رایانه‌ایاز جمله جرائم رایانه‌ای‌اند که در مقیاس بسیار کم در دهه ۱۳۷۰ واقع شده و با قوانین کیفری مرسوم مورد رسیدگی قرار گرفته اند. دادنامه مورخه ۷۲/۴/۳ شعبه ۶۵ دادگاه کیفری ۲ تهران یکی از نمونه آرایی است که مبین به کار گیری قوا نین کیفری سنتی در خصوص جرائم رایانه‌ای است.به موجب این دادنامه، دادگاه در خصوص شکایت یک شرکت نرم افزاری رایانه علیه مسئولین شرکت ایرانی دیگر مبنی بر تکثیر و فروش غیر مجاز نرم افزار رایانه‌ای، پس از احراز وقوع

۳۸- وزیر ازتباطات وفناوری اطلاعات(آقای احمد معتمدی) در مصاحبه مورخه ۸۳/۲/۲۷ باسایت آ.تی. ایران تعداد کاربران اینترنت در ایران را پنج میلیون نفر اعلام کرد.یعنی به ازای هر ده هزار نفر ۷۰۰نفر کاربر وجود دارد.

۳۹- دژپسند فرهاد،معاون وزیر بازرگانی،سایت اینترنتی WWW.ITIRan.com مصاحبه ۸۲/۲/۲۶

بزه به استناد بند ۱۱ ماده ۲۳ قانون حمایت از حقوق مؤلفان ومصنفان وهنر مندان مصوب ۱۳۴۸ متهم را به تحمل مجازات محکوم وحکم به جلو گیری از عرضه نرم افزارهایی که بطور غیر مجاز تکثیر شده اند صادر نموده است.[۴۰]

از نیمه دوم دهه ۱۳۷۰ وبالاخص از ابتدای دهه ۱۳۸۰ که استفاده از رایانه های شخصی توسط سازمانهای اداری و مؤسسات خصوصی و افراد حقیقی گسترش یافته دسترسی به خدمات متعدد اینترنت امکان پذیر شده است. ارتکاب جرائم رایانه‌ای نیز از رشد نسبتا سریعی برخوردار بوده است.اشاعه فحشا ومنکرات و انتشار عکس ها وتصاویر و مطالب خلاف عفت عمومی،ایجاد اختلاف بین اقشار جامعه از طریق طرح مسائل قومی و نژادی،انتشار مطالب نژاد پرستانه،انتشار اسناد ومسائل محرمانه،اهانت به مقدسات مذهبی و دینی،اهانت وافترا نسبت به مقامات دولتی و اشخاص حقیقی وحقوقی،سرقت ادبی وغیره از جمله جرائمی هستند که بعد از فراهم شدن امکان استفاده از خدمات اینترنت از طریق وب سایتها و وبلاگها،پست الکترونیک، گروه های خبری، چت(گپ زدن)و سایر سرویسهای اینترنت بوقوع پیوسته اند. قانونگذار درسال ۱۳۷۹ در برابر برخی از جرائم رایانه‌ای واکنش نشان داده و با الحاق تبصره ۳ به ماده ۱ قانون مطبوعات مقرر داشت «کلیه نشریات الکترونیکی مشمول مواد این قانون است.»

اولین واکنش قانونی کشور ما در برابر بعضی از جرائم رایانه‌ای قانون اصلاح قانون مطبوعات مصوب ۷۹/۱/۳۰ مجلس شورای اسلامی است که در تاریخ ۷۹/۲/۷ مورد تأیید شورای نگهبان قرار گرفته است.

دومین واکنش قانونی کشور ما در مقابل جرائم رایانه‌ای از طریق وضع «قانون حمایت از حقوق پدید آورندگان نرم افزارهای رایانه‌ای»بعمل آمد.این قانون در تاریخ ۷۹/۱۰/۴ به تصویب مجلس شورای اسلامی و در تاریخ ۷۱/۱۰/۱۰ به تأیید شورای نگهبان رسیده است.(۱)ماده ۱۳ قانون مذکور نقض دید آورندگان آن دسته از نرم افزارهای رایانه‌ای را که مورد حمایت این قانون قرار گرفته اند،جرم تلقی وبرای آن مجازاتی معادل ۹۱ روز تا شش ماه حبس و جزای نقدی تعیین کرده است. البته اشکلاتی بر این قانون وارد است که در این مقال نمی گنجد.

سومین عکس العمل قانونگذار ایران در مقابل جرائم رایانه‌ای در سال ۱۳۸۲ از طریق تصویب قانون مجازات جرائم نیروهای مسلح مصوب ۸۲/۱۰/۹ مجلس شورای اسلامی (۲) به عمل آمد. به موجب ماده ۱۳۱ این قانون جعل اطلاعات وداده‌های رایانه‌ای تسلیم و افشاء غیر مجاز اطلاعات وداده‌ها به افرادی که صلاحیت دسترسی به آن را ندارند،سرقت ویا تخریب حاملهای داده،وسوء استفاده مالی از طریق رایانه (کلاهبرداری واختلاس) توسط نظامیان جرم تلقی و مرتکب حسب مورد به مجازات جرم ارتکابی محکوم می‌شود.

چهارمین واکنش قانونی مرتبط با جرائم رایانه‌ای از طریق تصویب قانون تجارت الکترونیکی مصوب ۸۲/۱۰/۱۷ مجلس شورای اسلامی به عمل آمده است. به موجب مواد ۶۶،۶۷،۶۸،۶۹،۷۴،۷۵،۷۶ و۷۷ این قانون کلاهبرداری، جعل،ودستبابی وافشاء غیرمجاز اسرار تجاری نقض حقوق مربوط به مالکیت معنوی (کپی رایت) وغیره... که از طریق رایانه و در بستر تجارت الکترونیکی انجام شود جرم تلقی و برای آن مجازات تعیین گردیده است.

۴۰- خبرنامه انفورماتیک،ش۵۳،دبیرخانه شورای عالی انفور ماتیک،ص۲۷و۲۸

هر یک از چهار قانون فوق الذکر در بستر خاص خود قابلیت اعمال دارند. مثلا قانون مطبوعات صرفاً نسبت به جـرائم رایانـه‌ای ارتکابی در قالب نشریات الکترونیکی و قانون مجازات نیرو های مسلح صرفا در مورد بعضی از جرائم رایانه‌ای نظامیان و قـانون تجارت الکترونیکی فقط در مورد برخی از جرائم رایانه‌ای ارتکابی در بستر تجارت الکترونیکی قابل اجرا هستند.

برای مقابله با سایر سوء استفاده‌های رایانه‌ای مانند سوء استفاده از رایانه به منظور نفـوذ بـه حـریم خصوصـی افـراد، تخریـب، سرقت، و توقف و تغییر داده‌هایی که فاقد شرایط مقرر در قانون حمایت از حقوق پدیدآورندگان نرم افزارهای رایانه‌ای هسـتند، سوءاستفاده‌های مالی رایانه‌ای خارج از بستر تجارت الکترونیک وسایر سوء استفاده های رایانـه‌ای نیـاز بـه یـک قـانون جـرائم رایانه‌ای پیشرفته و جامع الاطراف می‌باشد.

شورای عالی توسعه قضایی قوه قضائیه پیش نویس قانون جرائم رایانه‌ای و آئـین دادرسـی آن را در سـال ۱۳۸۲ تهیـه و طـی جلسات متعددی از دی ماه تا اوایل خرداد ماه با حضور حقوقدانان و متخصصین امور رایانه آن را مورد بررسی قرار داد، تا پس از تصویب رئیس قوه قضائیه به عنوان لایحه جرائم رایانه‌ای از طریق هیئت دولت به مجلس شورای اسلامی تقدیم گردد.

مبحث دوم:تعریف جرم رایانه‌ای

ضرورت تعریف جرم رایانه‌ای

ارائه تعریف جرم رایانه‌ای از جهات متعدد ذیل دارای اهمیت است:

۱–ارائه یک تعریف استاندارد از جرم رایانه‌ای می‌تواند از لحاظ آموزشی در تعلیم و تعلم و تشـحیذ ذهـن دانشـجویان و اسـاتید وکلیه کسانی باشد که به دنبال فراگیری مطالبی در این خصوص هستندموثر و مفید واقع شود.

۲–چنانچه یک تعریف واحد و یا تعاریفی که از لحاظ ماهوی دارای تفاوت اساسی نباشند از جرم رایانه‌ای نداشته باشـیم،کاربران فناوری اطلاعات و مقامات مجری قانون (مقامات تحقیق و تعقیب وقضات دادگاه‌ها) در وضعیتی نا مشـخص و فضـایی مـبهم قرار گرفته نمی‌توانند تکالیف و وظایف قانونی خود را به نحو مطلوب انجام دهند.

۳–بدون تعریف جرم رایانه‌ای جمع آوری اطلاعات آماری معنی دار که می تواند به منظور تجزیه و تحلیل ساختارها و الگو های جرم استفاده شود،غیر ممکن خواهد بود.

۴–ارائه یک تعریف معین از جرم رایانه‌ای وهمچنین ارائه داده‌های آماری و اطلاعات صحیح مبتنی بر یک تعریف معـین بـرای آموزش عمومی افراد جامعه به منظور مقابله با تهدیدات و جلو گیری از ارتکـاب جـرم از طریـق توسـعه طرحهـای حفـاظتی و بازدارنده ضروری است.

۵–به لحاظ فراملی بودن جرم رایانه‌ای تعریف معین از جرم رایانه‌ای میتواند در انجام معاضدت قضایی و همکـاری هـای بـین المللی برای مبارزه با جرم رایانه‌ای مؤثر باشد.

تعاریف مختلف و علت‌های آن

با این حال تا کنون تعاریف گوناگونی از جرم رایانه‌ای از سوی سازمانهای بین‌المللی، قانونگذاران،مراجع رسـمی و غیـر رسـمی برخی از کشورها ومتخصصان حقوق اطلاعات کیفری ارائه شده است. و هنوز اجماع بین المللـی بـرای تعـاریف جـرم رایانـه‌ای وجود ندارد. این امر ناشی از عوامل مختلفی است. یکی از این عوامل تفاوت سطوح کاربری وبهره برداری از فنـاوری اطلاعـات در کشورهای مختلف است.عامل دیگر نظریات و دیدگاهها و رهیافت های مختلفی هستند که مبنای تعاریف جرم رایانه‌ای قـرار

گرفته اند. عامل سوم تفاوت در نظام حقوق کیفری کشورهای مختلف است که موجب می شود در مقابل یک پدیده نوظهور واکنشهای متفاوتی از نظامهای حقوقی مختلف بروز کند. در برخی از کشورها فناوری اطلاعات علاوه بر ایجاد زمینه سوء استفاده های جدیدی که مستلزم جرم انگاری و وضع قوانین کیفری جدیدی است،کیفیت ارتکاب جرائم سنتی را به نحوی تغییر داده است که موجب تغییر در ماهیت این جرائم گردیده و در نتیجه اصلاح قوانین کیفری موجود را اجتناب ناپذیر نموده است. در برخی دیگر از کشورها مانند فرانسه قوانین کیفری گذشته به نحوی تنظیم شده اند که استفاده از رایانه و یا سایر مظاهر فناوری اطلاعات تغییری در ماهیت اینگونه جرائم نداده است. قانون جرائم رایانه‌ای۱۹۸۸ فرانسه شامل پنج عنوان جرم رایانه‌ای می شد که یک عنوان شامل جرم جعل رایانه‌ای بود. درسال ۱۹۹۴ با این استدلال که بزه جعل در ماده ۱-۴۴۱ کد کیفری فرانسه دارای آنچنان کلیتی است که جعل در محیط انفور ماتیک را نیز شامل می شود. عنوان مجرمانه جعل رایانه‌ایبه عنوان یک بزه مستقل زائد تشخیص داده شد ونسخ گردید و در گزارشات رسمی دولت بر این امر تصریح شده بود که مقررات سنتی قابل سرایت به شبکه های اطلاعاتی نیز هست. [۴۱]

تفاوت در تعریف جرم رایانه‌ایموجب اختلاف در تعیین مصادیق آن شده است.بدین نحو که بعضی از تعاریف موسع بوده شامل طیف گسترده ادبی از اعمال مجرمانه وسوء استفاده های رایانه‌ای می گردد و در مقابل بعضی از تعاریف مضیق بوده مصادیق کمتری را در بر خواهد گرفت.با ذکر این مقدمه به بررسی وتجزیه وتحلیل تعاریف مختلف جرم رایانه‌ایمی پردازیم. دراین مبحث ابتدا اقدامات سازمانهای بین المللی در خصوص تعریف جرم رایانه‌ای مورد بررسی قرار می گیرد،سپس به بررسی تعریف این جرم از دیدگاه متخصصین و حقوق چند کشور می پردازیم.

الف)اقدامات انجام شده ازسوی سازمانهای بین المللی در مورد تعریف جرم رایانه‌ای

۱- تعریف OECD از جرم رایانه‌ای

اولین اقدام برای تعریف جرم رایانه‌ای از سوی سازمان همکاری و توسعه اقتصادی (OECD) صورت گرفت. اما گروه متخصصان این سازمان در سال ۱۹۸۳ به جای تعریف جرم رایانه‌ای سوء استفاده رایانه‌ای را به شرح زیر تعریف کرده اند:

«سوء استفاده از رایانه شامل هر رفتار غیر قانونی،غیر اخلاقی یا غیر مجاز مربوط به پردازش خودکار و انتقال داده‌ها است.» [۴۲]

پرفسور زیبر آلمانی در تأیید این تعریف می گوید:

«امروز اجماع بین الملل بر این است که جرم رایانه‌ای باید بطور موسع تعریف شود ...مطالعات اخیر مفاهیم وسیع تر وپیشرفته تر را از مجرمیت داده‌ها ویا جرم اطلاعاتی ارائه می کند.ارائه این گونه تعریف ها موجب می شود بتوان ازآنها در مطالعات مختلف جرم شناختی،جرم یابی،اقتصادی باز دارنده یا قضایی استفاده کرد.واضح است که تعاریف تخصصی تر وبا طبقه بندی جزئی تراز پدیده جرم رایانه‌ای وجود دارد واین امر منوط به هدف تحقیقاتی مورد نظر است تبعا طبقه بندی های تکنیکی در کنار تفاوت های جامعه شناختی تنها ارزش محدودی برای مطالعات قضایی دارد.» [۴۳]

۴۱- جور ابراهیمیان،نجات،جزوه جرائم رایانه ای در حقوق فرانسه، کمیته مبارزه باجرائم رایانه ای شورای عالی توسعه قضایی ۱۳۸۲

۴۲- دزیانی محمد حسن ابعاد جزایی کاربرد کامپیوتر،خبرنامه انفورماتیک،ش۵۸،ص۱۵۷

۴۳- زیبر،اولریش،پیدایش بین المللی حقوق اطلاعات کیفری،ترجمه دزیانی،جزوه جرائم کامپیوتری،ج۳،شورای عالی انفورماتیک،۱۳۷۶ ص۱۶

یکی از محققین در مقام نقد تعریف (OECD) گفته است:

«در این تعریف اولا ذکر عبارت رفتار غیر قانونی کفایت می کند. درحقوق جزا رفتاری که جرم شناخته می شود باید در قانون ذکر شود (عنصر قانونی).از این رو ذکر قید غیر قانونی بودن در تعریف کفایت می کند وذکر دو عنوان دیگر یعنی غیر اخلاقی وغیر مجاز خالی از اشکال نیست.

ثانیا،جرم در قانون تصریحا تعیین می شود اما رفتار غیر مجاز گاهی می تواند جرم باشد وگاه دارای وصف غیر مجرمانه است.خواه این توصیف غیر جزایی بتواند داخل در مفاهیم و اعمال مسئولیت آفرین درحقوق مدنی جای گیرد و خواه درحقوق اداری جاری مجرایش باشد. به هر حال ذکر عبارت غیر قانونی ذات و اساس جرم را می‌رساند اما عمل غیر مجاز دایره‌ای وسیع تر از مفهوم جرم دارد.عبارت غیر اخلاقی نیز چنین است.

ثالثا،جزء مسائلی که در توصیه های سازمان ملل وحتی در توصیه های خود آقای زیبر و همگنان وی ذکر شده استفاده از حقوق جزا به عنوان آخرین راه حل است.تا وقتی بتوان عمل را داخل در مفاهیم مسئولیت مدنی وتخلفات اداری طرح کرد جرم شناختن آن کاری غیر عقلایی است که ذکر دلایل این عدم منفعت عقلایی نیازمند بحث های تفضیلی است.تعریف موسع (OECD) در تناقض با اصل«حقوق جزا به عنوان آخرین راه حل» است.

رابعا، از جمله مسائل مهم که سالهای اخیر در سیاست جنایی طرح می شود مسئله اجتناب از تورم کیفری است. با انباشتن انبان حقوق جزا از جرائم مختلف وجرم شناختن هر عملی بدون توجه به پیامدها یا سود مندی آن این کار عملی لغو می نماید. این تعریف در تضاد با این اصل نیز هست.

خامسا، عبارت پردازش اتوماتیک یا انتقال داده‌ها نیز نارسا است متخصصان (OECD) دربخش اول تعریف راه وسیع نگری در پیش گرفته‌اند اما دربخش دوم تعریف نحوه ارتکاب یا موضوع ارتکاب را بسیار محدود کرده اند. محدودیتی که موجب دور افتادن از برخی لوازم بحث است با تنوعی که در اشکال مجرمانه جرم رایانه‌ای قابل مشاهده است،انحصار تعریف برداده پردازی اتوماتیک یا انتقال داده‌ها امر غیر معقول است.[۴۴]»

علی رغم انتقادهایی که از ناحیه حقوقدانان به این تعریف وارد شده است،به نظر می رسد کهOECD در مقام تعریف جرم رایانه‌ای نبوده،بلکه در مقام بیان انواع سوء استفاده های رایانه‌ای بوده است که نهایتا آنها را به سه دسته ۱-غیر قانونی ۲-غیر اخلاقی ۳-غیر مجاز طبقه بندی کرده است.دلیل بر این ادعا این است که سازمان مذکور در سال ۱۹۸۵ لیستی از اعمال مجرمانه را به عنوان مبنای مشترک ارائه داد و پیشنهاد کرد که کشورهای عضو از طریق تقنین جزایی ملی آنها راجرم انگاری کنند.

اگر سازمان همکاری وتوسعه اقتصادی OECD هر نوع سوء استفاده غیر اخلاقی و غیر مجاز رایانه‌ای را جزء تعریف و مصادیق جرم رایانه‌ای تلقی می کرد لازم نبود از کشورهای عضو بخواهد به عنوان مبنای مشترک از طریق تقنین جزایی با این اعمال مجرمانه مقابله شود. بنابراین تعریف OECD از سوء استفاده رایانه‌ای نمی‌تواند به عنوان تعریف جامع و مانع جرم رایانه‌ای در نظام حقوقی ما قابل استفاده باشد. البته ممکن است گفته شود، متخصصان OECD نمایندگان نظامهای حقوقی مختلف اعم از حقوق نوشته وحقوق کامن لاو و... هستند و در نظام حقوقی کامن‌لا و اصل قانونی بودن جرم و مجازات حاکم

۴۴- دزیانی محمد حسن، جزوه جرائم کامپیوتری، ج۲، شورای عالی انفور ماتیک ۱۳۷۶،ص۱۱و۱۲

نیست. علی هذا ممکن است یک سوء استفاده رایانه‌ای بدون اینکه بوسیله قانون نوشته ممنوع شده باشد، در یک کشور تابع حقوق کامن‌لاو غیر مجاز تلقی وجرم محسوب شود.پس نتیجه گیری می شود که متخصصان OECD خواسته اند تعریفی ارائه دهند که شامل جرم رایانه‌ای در همه نظامهای حقوقی شود. این استنباط اگر چه با پیشنهاد OECD به کشورهای عضو مبنی بر برخورد کیفری تقنینی با پنج مورد خاص از سوء استفاده‌های رایانه‌ای به عنوان مبنای مشترک مغایرت دارد، اما قابل تأمل است.

۲- نظر شورای اروپا درمورد تعریف جرم رایانه‌ای

دومین سازمانی که تلاشهایی را برای تعریف جرم رایانه‌ای به عمل آورد شورای اروپا بود.کمیته متخصصان جرم رایانه‌ای که توسط کمیته اروپایی مشکلات ناشی از جرم وابسته به شورای اروپا، از سال ۱۹۸۵ تشکیل گردیده بود، در سال۱۹۸۹ یک توصیه نامه و یک گزارش ارائه کرد که در اجلاس معاونین وزراء شورای اروپا تصویب شد.این توصیه نامه که R (۸۹) نامیده می‌شود، بدون اینکه تعریفی از جرم رایانه‌ای ارائه کند، خطوط راهنمایی را برای دول عضو تعیین کرد. این خطوط راهنما شامل یک فهرست حداقل و یک فهرست اختیاری از جرائم رایانه‌ای بود .فهرست حداقل شامل اعمالی می شد که جرم بودن آنها مورد اجماع اعضا بود. فهرست اختیاری جرائم رایانه‌ای شامل اعمالی می‌شد که جرم بودن آنها مورد اجماع نبود. در توصیه نامه R(۸۹) از کشورهای از کشورهای عضو خواسته شده بود که نسبت به جرم انگاری فهرست حداقل اقدام نمایند. فهرست حداقل جرائم ضروری برای یکنواخت کردن سیاست جنایی مربوط به تقنین جرم رایانه‌ای شامل هشت عنوان مجرمانه و فهرست اختیاری شامل چهار عنوان مجرمانه بود.

کمیسیون متخصصان جرم رایانه‌ای شورای اروپا در گزارش توجیهی توصیه‌نامه R (۸۹) اعلام می‌دارد:

«هر کوششی برای تعریف کردن جرم رایانه‌ای با نوعی نارسایی روبرو می‌شود. عیب تعریف OECD این است که شامل رفتارهای غیر مجاز و غیر اخلاقی نیز می‌شود.اگر چه آن رفتار ممکن است جرم نباشد. از سویی تعریف‌های ارائه شده چون اکثرا جرائمی را شامل می‌شود که ضرورتاً جرم رایانه‌ای در معنای مضیق نیستند، محل تردید است. این ملاحظات و دیگر مسائل موجب شد که کمیسیون‌ها همان رهیافت OECD را انتخاب کند بدون اینکه بخواهد تعریفی مستقل از جرم رایانه‌ای ارائه کند.»[۴۵] دربند ۲۸ گزارش توجیهی توصیه نامه R(۹۵) مصوب سال ۱۹۹۵

شورای اروپا در گزارش توجیهی توصیه نامه R(۹۵) مصوب سال ۱۹۹۵ اصطلاح جرم فناوری اطلاعات را به جای اصطلاح جرم رایانه‌ای به کار برده و گفته است مفهوم جرائم مربوط به رایانه برای اهداف توصیه نامه (۸۹)R که فهرستی ازاعمال مجرمانه ویژه را دربردارد طرح گردیده است. در بند ۲۸ گزارش مذکور تصریح گردیده تعریف کردن جرم مربوط به رایانه به عنوان طبقه ویژه‌ای ازجرم بسیار مشکل است. دربندهای ۲۹و ۳۰گزارش مذکورعلت استفاده از اصطلاح جرم فناوری اطلاعات به جای اصطلاح جرم رایانه‌ای بیان شده است و درتفسیرخود از واژه فناوری اطلاعات وسیع‌ترین معنای ممکن را برای این واژه در نظر گرفته است.

متن بندهای ۲۹و۳۰گزارش توجیهی توصیه نامه R(۹۵) به شرح زیر است:

۴۵- پاکزادبتول،جرائم کامپیوتری، پایان نامه کارشناسی ارشد، دانشگاه شهید بهشتی،۱۳۷۵،ص۳۴

«۲۸–در توصیه نامه شماره R(۸۹) عبارت جرم مربوط به رایانه به کار رفته است، چنین تشخیص داده شده که تعریف کردن جرائم مربوط به رایانه به عنوان تیپ یا طبقه ویژه از جرم به اندازه طبقات موجود جرم در قوانین جزایی خیلی مشکل است اگرچه غیر ممکن نیست.

این واقعیت که در طی ارتکاب یک جرم مرتکب از یک سیستم رایانه‌ای یا از تسهیلات دیگر فناوری اطلاعات استفاده کرده است شاید همیشه عنصر تعیین کننده ای برای تعریف چنین جرمی به عنوان جرم مربوط به رایانه نباشد. بنا بر این برای هدف های توصیه‌نامه شماره R (۸۹) مفهوم جرائم مربوط به رایانه با تعریف فهرست کاملی از اعمال ویژه که پیشنهاد شده است به عنوان اعمال مجرمانه محسوب شوند طرح شده است.

۲۹–در این توصیه نامه [به جای اصطلاح جرم رایانه‌ای] اصطلاح جرم فناوری اطلاعات بکار می‌رود اما در این زمینه این ایده باید در وسیع‌ترین معنای ممکن درک شود.

۳۰–جرائم مربوط به فناوری اطلاعات (که از این به بعد جرائم فناوری اطلاعات) نامیده می‌شود را می‌توان به وسیله یک سیستم رایانه‌ای مرتکب شد. اما سیستم می‌تواند هم هدف وهم محیط جرم باشد. بعلاوه آن سیستم‌هایی که حتی عنصری از ارتکاب جرم نیستند اما به سادگی تشکیل دهنده محیطی هستند که درآن ادله هرجرمی را می‌توان یافت،جزء این گروه هستند. بنا براین، این توصیه‌نامه در زمینه موضوعات آئین دادرسی کیفری به «جرائم مربوط به فناوری اطلاعات »به عنوان در برگیرنده هرگونه جرم کیفری اشاره می‌کند که برای تحقیقات مربوط به آن مقامات تحقیق باید به اطلاعاتی دستیابی پیدا کنند که در سیستم‌های رایانه‌ای (سیستم های پردازش داده الکتریکی) پردازش یا منتقل شده اند.»

نکته بسیار ظریفی در مطالب مطروحه در بندهای ۲۸،۲۹و۳۰ گزارش توجیهی توصیه نامه R(۹۵) شورای اروپا وجود دارد وآن نکته این است که متخصصان جرائم رایانه‌ای شورای اروپا و سایر سازمانهای بین المللی وقتی که در جایگاه تعیین معیار برای جرم انگاری در زمینه جرائم رایانه‌ای بوده‌اند. نتوانسته‌اند معیار دقیقی برای جرم رایانه‌ای ارائه دهند که بتوان بوسیله آن مصادیق جرائم رایانه‌ای را تعیین نمود. لذا در این مقام صرفاً به معرفی مصادیقی از جرم رایانه‌ای به عنوان مبنای مشترک اکتفا کرده‌اند. اما وقتی که در مقام وضع مقرراتی برای رسیدگی به جرائم رایانه‌ای هستند در وسیعترین معنای ممکن به این مسئله نگریسته و حتی جرمی را که رایانه نقشی در تحقق عنصر مادی آن نداشته و صرفا دلایل مربوط به آن در سیستم های رایانه‌ای پردازش یا منتقل شده باشد با جرائمی که در آنها رایانه هدف و یا ابزار جرم است تحت یک عنوان به نام «جرائم فناوری اطلاعات»جمع کرده اند.

۳- نظرسازمان ملل درخصوص تعریف جرم رایانه‌ای

سازمان ملل در نشریه شماره ۴۴ خود (نشریه بین المللی سیاست جنایی)با ذکر این نکته که تعریف مورد توافقی در خصوص جرم رایانه‌ای وجود ندارد و شاید نتوان ارائه کرد، جرم رایانه‌ای را شامل فعالیتهای مجرمانه با ماهیت سنتی مانند سرقت و جعل ویا با ماهیت نوین یعنی راههای تازه برای سوء استفاده بیان می کند.تصریح به جا و به موقع سازمان ملل مبنی بر اینکه باید جرم رایانه‌ای گفت نه سوء استفاده از رایانه،از نکات بسیار مهم است.[۴۶]

۴۶– نشریه بین المللی سیاست جنایی سازمان ملل شماره های ۳۳و۳۴،ترجمه دزیانی، جزوه جرائم کامپیوتری،جلد یک،ص،شورای عالی انفورماتیک۱۳۷۶

٤- نظر AIDP در خصوص تعریف جرم رایانه‌ای

انجمن بین المللی حقوق جزا (AIDP) نیز در نشست خود درسال ۱۹۹۲ در دانشگاه ورتسبورگ آلمان نتوانست تعریفی استاندارد برای جرم رایانه‌ای ارائه دهد. همه شرکت کنندگان به توافق رسیدند به جای تعریف جرم رایانه‌ای، فهرست حداقل جرائم رایانه‌ای مقرر در توصیه نامه R(۸۹) مشروط بر اینکه به صورت عمدی ارتکاب یابند، به عنوان مبنای مشترک پذیرفته شود. این انجمن درنشست سال ۱۹۹۴ خود در ریودوژانیرو نیز بدون اینکه موفق به ارائه تعریفی در این خصوص شود، توصیه کرد که کشورهای عضو علاوه بر فهرست حداقل جرائم رایانه‌ای مقرر در توصیه نامه R(۸۹) شورای اروپا چهار عمل مجرمانه دیگر را به عنوان جرم رایانه‌ای جرم انگاری نماید.

٥- تعریف جرم رایانه‌ای و کنوانسیون جرائم سایبر

کنوانسیون جرائم سایبر یک سند بین‌المللی است که موضوع آن جرائم رایانه‌ای می‌باشد. این کنوانسیون در سال ۲۰۰۱ در یک کنفرانس بین‌المللی که با حضور ۲۴ کشور عضو شورای اروپا و چهار کشور آمریکا، ژاپن، کانادا، و آفریقای جنوبی در شهر بوداپست تشکیل شده بود به تصویب رسید. در این کنوانسیون نیز جرم رایانه‌ای تعریف نشده است ولی مصادیق بیشتری تحت عنوان جرم سایبر ذکر شده و از کشور های عضو خواسته شده است که نسبت به جرم انگاری آنها از طریق قوانین کیفری خود اقدام کنند.

در بند ۳۴ گزارش توجیهی این کنوانسیون آمده است:«جرائم مندرج در کنوانسیون نشانگر یک توافق حداقل است که از بسط و توسعه آن در حقوق داخلی ممانعت نمی‌کند. این امر تا حد زیادی مبتنی بر راهبردهای توصیه شماره R(۸۹) شورای اروپا پیرامون جرائم مربوط به رایانه وعملکرد دیگر سازمانهای بین المللی عمومی وخصوصی (سازمان ملل متحد،انجمن بین المللی حقوق جزا،و سازمان همکاری وتوسعه اقتصادی) است،اما تجارب پیشرفته تری که از برخورد با سوء استفاده از توسعه شبکه های ارتباط راه دور حاصل شده است رانیز دربر می‌گیرد.»

علی رغم اینکه شورای اروپا در توصیه نامه R (۸۹) اصطلاح «جرائم مربوط به رایانه» و در توصیه نامه شماره R (۹۵) «جرائم فناوری اطلاعات» را به کار برده بود در این کنوانسیون که قبل از طرح در کنفرانس به تصویب شورای اروپا رسیده است اصطلاح «جرم سایبر» به کار رفته وجرائم مرتبط با رایانه یکی از پنج گروه جرائمی است که ذیل عنوان جرم سایبر از آنها نام برده شده است.

ب) تعریف جرم رایانه‌ای از دیدگاه حقوقدانان و حقوق چند کشور

۱- تعریف جرم رایانه‌ای از دیدگاه حقوقدانان و حقوق آمریکا

پرفسور ادوارد ام وایز استاد دانشگاه میشیگان آمریکا در گزارشی که در مورد جرائم رایانه‌ای آمریکا برای انجمن بین‌المللی حقوق جزا تهیه کرده نوشته است «؛هیچ تعریفی ازجرم رایانه‌ای وجود ندارد که مورد قبول همه واقع شود.اکنون هریک از ایالتهای آمریکا یک قانون مخصوص به خود دارند که بویژه جرائمی را مورد بررسی قرار می‌دهند که متضمن رایانه است.آمریکا یک قانون فدرال هم دارد. جرائم رایانه‌ای را می توان به عنوان نقض یکی از این قوانین جرائم رایانه‌ای تعریف کرد، اما شمول این قوانین یکسان نیست.اینکه هرکس یک اصطلاح را چگونه تعریف می‌کند به این بستگی دارد (یا باید

بستگی داشته باشد)که هدف وی از تعریف آن چیست. به نظر می‌رسد که هدف از تلاش برای مجزا کردن جرائم رایانه‌ای به عنوان یک پدیده متمایز است که نقاط آسیب‌پذیر ویژه که در نتیجه وابستکی به تکنولوژی رایانه‌ای ایجاد شده اند شناسایی شوند. این امر هدفی است که در تعریف سازمان همکاری و توسعه قضایی دیده می شود. حتی تعریف این سازمان گرچه وسیع است ولی در دو جنبه تمام جرائم مربوط به رایانه را دربر نمی گیرد.

۱-شامل سرقت سخت افزار یا تجهیزات دیگر مانند دیسکت های خالی وتخریب آنها نمی‌شود

۲-شامل مواردی که رایانه برای کمک و ارتکاب جرم به کار می رود نمی شود.»[۴۷]

جیمز رابینسون حقوقدان آمریکایی دیگر،در کنفرانس جرائم رایانه‌ای بین‌المللی اسلو در ماه می سال ۲۰۰۰ در خصوص مفهوم جرم رایانه‌ای می‌گوید: «رفتار مجرمانه علیه رایانه به سه شکل صورت می پذیرد:

۱-گاهی رایانه هدف یک جرم است به عبارت بهتر رایانه موضوع جرم قرار می‌گیرد. مثل سرقت اطلاعات یا خدمات رایانه‌ای، هک کردن، خرابکاری رایانه‌ای (سابوتاژ) و.....

۲-گاهی رایانه به عنوان وسیله ارتکاب جرم است. مانند کلاهبرداری رایانه‌ای، جعل رایانه‌ای، پورنوگرافی اطفال...

۳-گاهی نیز رایانه وسیله یا هدف مستقیم جرم نیست بلکه به انضمام یک جرم دیگر در مسیر رفتار جنایی قرار می گیرد. مثل ذخیره کردن پورنوگرافی های اطفال توسط پدو فیلی ها یا ذخیره سلزی اطلاعات غیر مجاز که از رایانه یا منبع دیگری حاصل شده است.یعنی رایانه در اینجا ممکن است بعد از حصول نتیجه مجرمانه فعل ذیگری وارد صحنه کیفری شود.[۴۸]

وزارت دادگستری آمریکا جرم رایانه‌ای را اینگونه تعریف کرده است:«هر اقدام غیر قانونی که برای ارتکاب،پی جویی،یا پی گرد قضایی آن بهره برداری از دانش فناوری رایانه ضروری باشد جرم رایانه‌ای است.»[۴۹]

۲- تعریف جرم رایانه‌ای از دیدگاه حقوقدانان و حقوق کانادا

دکتر پیرا گوف درگزارشی که برای انجمن بین المللی حقوق کیفری پیرامون جرائم رایانه‌ای در کانادا تهیه کرده، گفته است: «اصطلاح جرم رایانه‌ای که اخیرا مطرح شده گمراه کننده است.در بسیاری از موارد جرم رایانه‌ای به وضوح وبطور قانونی از جرائم موجود همچون سرقت،جعل،کلاهبرداری وایجاد خسارت کیفری جدا نیست. بسیاری از سوء استفاده های رایانه‌ای را می توان در قوانین کیفری متداول جای داد کارمند بانک که وجوه حسابهای دیگر را به حساب مخصوص منتقل وآن را برداشت میکند مرتکب سرقت شده است و رایانه را برای ارتکاب جرم مورد نظرش به کار گرفته است.در حال حاضر مقررات موجود در مورد سرقت وکلاهبرداری باید برای بحث جرائم رایانه‌ای مربوط کافی باشند باید در اینگونه موارد توجه داشت که رایانه وسیله مساعدت در ارتکاب جرم است ونه جرم رایانه‌ای درمعنای مصطلح»[۵۰]. مطابق تعریف دیگری درحقوق کانادا «جرم رایانه‌ای شامل هر نوع فعالیت مجرمانه است که دربرگیرنده کپی،استفاده،جابجایی،ملاحظه،دسترسی،یا سوء استفاده از سیستم‌های رایانه‌ای، عملکرد رایانه،داده‌ها یا برنامه های رایانه‌ای است.»[۵۱]

۴۷- جعفر پور ناهید، ترجمه جزوه جرائم کامپیوتری ودیگر جرائم علیه تکنولوژی اطلاعات در آمریکا، شورای عالی انفور ماتیک،۱۳۷۶

۴۸- جزوه گزارش توجیهی کلاهبرداری رایانه ای،شورای عالی توسعه قضایی،سال۸۲،ص۱و۲

۴۹- پرویزی رضا،جزوه جرائم کامپیوتری،شورای عالی توسعه قضایی ۱۳۸۲،ص۶

۵۰- پاکزاد بتول، همان،ص۳۵

۵۱- شریفی مرسده،جرائم کامپیوتری در حقوق جزای بین الملل،رساله کارشناسی ارشد،دانشگاه آزاد اسلامی تهران،ص۸۰

۳- تعریف جرم رایانه‌ای از دیدگاه حقوقدانان و حقوق آلمان

دکتر مونشلاگر در گزارشی که پیرامون جرائم رایانه‌ای در آلمان برای انجمن بین‌المللی حقوق جزا تهیه کرده، نوشته است:«تاکنون در مورد این اصطلاح تعریفی واحد که مورد پذیرش همگان باشد بدست نیامده وتعریف قضایی ساده‌ای در این زمینه وجود ندارد. بطور کلی همه اعمال مجرمانه ای که رایانه، ابزار یا وسیله دستیابی به هدفهایی قرار گرفته است به نظر من در این اصطلاح می گنجد. در استفاده از رایانه برای ارتکاب جرم،نه می توان این واقعیت را که جرم ارتکاب یافته است نادیده انگاشت، و نه این عمل اثری بر روی طبقه بندی جرم ارتکاب یافته دارد. البته ممکن است اثری بالقوه یا بالفعل در جهات قانون شکنی داشته باشد وهمین موجب می شود که کشف و تعقیب آن دچار مشکلاتی شود.»[۵۲]

گروه کاری پلیس فدرال و ایالتی به این نتیجه رسیدند که باید تعریفی مبتنی بر جرم شناسی،پیرامون جرائم رایانه‌ای ارائه داد. طبق تعریف ارائه شده جرائم رایانه‌ای شامل همه شرایطی است که پردازش الکترونیک داده‌ها وسیله یا موضوعی برای ارتکاب جرم یا تخلف باشد و بیانگر دلایلی برای ظن به ارتکاب جرم است.

٤- تعریف جرم رایانه‌ای از دیدگاه حقوقدانان و حقوق اتریش

پرفسور شیک در گزارش خود پیرامون جرائم رایانه‌ای اتریش به انجمن بین‌المللی حقوق جزا اظهار داشته: «به هنگام بررسی مفهوم جرم رایانه‌ای در اتریش آنچه در ابتدا جلب نظر می‌کند این است که در تعریف و تعیین این مفهوم و مفاهیم مرتبط با آن از دیدگاه‌های آلمان تبعیت زیادی شده است. بطور کلی جرم رایانه‌ای عبارت است از هر عمل مجرمانه‌ای که رایانه وسیله ارتکاب یا راه ارتکاب آن باشد.»[۵۳]

۵- تعریف جرم رایانه‌ای از دیدگاه حقوقدانان و حقوق ژاپن

دکتر آتسوشی یا ماگوچی در مقاله خود تحت عنوان جرائم رایانه‌ای و دیگر جرائم علیه فناوری اطلاعات در ژاپن که برای انجمن بین‌المللی حقوق جزا تهیه کرده، نوشته است: «نمایندگی پلیس ملی ژاپن تعریف رسمی جرم رایانه‌ای را چنین مطرح کرده است: جرائمی که شامل اعمال توأم با بی‌مبالاتی یا حوادثی هستندکه عملکرد یک سیستم رایانه‌ای را مختل می‌سازد و یا آن را مورد استفاده غیر قانونی قرار می‌دهد.جرائم رایانه‌ای نامیده می‌شوند.

جرائمی که تا سال ۱۹۹۰ برای پلیس ژاپن شناخته شده‌اند عبارتند از: ۱ - تخریب سخت افزار ۲- تخریب نوارها و دیسکت ها ۳-کذب سازی یا محو داده‌ها ۴- استفاده غیر قانونی از سخت افزار ۵- سرقت داده‌ها و برنامه‌ها.

در ژاپن برداشت پول نقد از یک ماشین تحویل‌دار اتوماتیکی یا استفاده متقلبانه از یک کارت پرداخت یا یک کارت بانکی که معمول‌ترین شکل جرم رایانه‌ای است، به عنوان سرقت مورد مجازات قرار می‌گیرد و طبق سیستم طبقه بندی نمایندگی پلیس ملی تحت عنوان جرائم رایانه‌ای طبقه بندی نمی‌شود، بلکه تحت عنوان جرائم مربوط به کارت‌ها گروه بندی می‌گردد.

در ژاپن چهار دسته جرم رایانه‌ای وجود دارد ۱-سرقت داده‌های رایانه‌ای ۲- سوءاستفاده از داده‌های رایانه‌ای ۳-استفاده غیر مجاز از یک رایانه ۴-سابوتاژ رایانه‌ای.[۵۴]»

۵۲- پاکزاد بتول،همان،ص۳۵

۵۳- شریفی مرسده،همان،ص۸۰

۵۴- جرم کامپیوتری و دیگر جرائم علیه تکنولوژی اطلاعات در ژاپن، ترجمه ناهید جعفر پور،جزوه جرائم کامپیوتری،ج۴،شورای عالی انفورماتیک، سال۷۶،ص۳۶

۶- تعریف جرم رایانه‌ای از دیدگاه حقوقدانان و حقوق هلند

پرفسور هنریک کاسپرسن استاد دانشگاه آمستردام در گزارشی که تحت عنوان جرائم رایانه‌ای و دیگر جرائم علیه تکنولوژی اطلاعات هلند برای انجمن بین‌المللی حقوق جزا نوشته است، می‌گوید: «درهلند پذیرفته شده که به ندرت می‌توان تعریف رضایت بخشی در مورد جرائم رایانه‌ای ارائه کرد، زیرا اگر تعریفی به وسیله اصطلاحات خیلی کلی فرموله شده باشد فاقد ارزش توضیحی است و اگر دارای اصطلاحات اختصاصی باشد خیلی مضیق و محدود می‌شود.

کمیته مشورتی جرائم رایانه‌ای هلند در سال ۱۹۸۷ جرائم رایانه‌ای را تعریف نکرد اما به هر حال طبق متد بکار گرفته شده می‌توان نتیجه گرفت که از نظر کمیته مذکور جرم رایانه‌ای هر رفتاری با قصد مجرمانه است که موجب صدمه به منافع خاص ناشی از پردازش اتوماتیک داده‌ها باشد این منافع به عنوان قابلیت دسترسی، تمامیت، و محدودیت تجهیزات رایانه‌ای و داده‌ها توصیف شده‌اند.

تعریف دیگری نیز ارائه شده است مثلا دپارتمان اطلاعات پلیس جرائم رایانه‌ای گزارش شده توسط پلیس محلی را از سال ۱۹۸۴ طبق تعریف زیر ثبت می کند:

جرم مربوط به رایانه یعنی رفتاری که (بطور بالقوه) مضر است و به واسطه‌هایی مربوط می شود برای ذخیره سازی، پردازش یا انتقال داده‌ها از رایانه کمک می گیرند.

پلیس این جرائم را به دو دسته تقسیم کرده است:

۱-زمانی که رایانه به منزله هدف جرم باشد

۲- زمانی که رایانه به منزله وسیله جرم باشد. »[۵۵]

۵۵- ر.ک. جرم کامپیوتری و دیگر جرائم علیه تکنولوژی اطلاعات در هلند،ترجمه ناهید جعفر پور،جزوه شورای عالی انفورماتیک،سال۷۶

مبحث سوم طبقه بندی جرائم رایانه‌ای

شناخت طبقات و انواع مختلف جرائم رایانه‌ای علاوه بر این که طریقی آسان و مطمئن برای شناخت ماهیت این جرائم است، می‌تواند کمک مؤثری برای مقابله با مشکلات ناشی از این جرائم باشد با توجه به محورهای مختلفی که برای طبقه بندی وجود دارد می توان طبقه بندی های متفاوتی را از جرائم رایانه‌ایارائه نمود. در این مبحث آن دسته از طبقه بندی ها را که در شناخت ماهیت این جرائم و ارائه راههایی برای مقابله با آن مؤثر باشد مورد بررسی قرار می‌دهیم. به لحاظ خصیصه فراملی جرائم رایانه‌ای کوششهایی توسط سازمانهای بین‌المللی برای طبقه بندی این جرائم به عمل آمده است تا با ارائه به کشورها اجماعی بین‌المللی در خصوص شناخت ماهیت و راه‌های مقابله با این جرائم حاصل شود. کشورهای توسعه یافته و برخی از کشورهای در حال توسعه نیز که پیشرفتی در زمینه کار برد فناوری اطلاعات دارند و در نتیجه با طیفهای مختلفی از جرائم رایانه‌ای مواجه بوده‌اند، به فراخور موقعیت و وضعیت فنی و حقوقی خود اقدام به طبقه بندی این جرائم کرده‌اند.در این مبحث ابتدائا به بررسی برخی از نوشته‌ها و اقدامات به عمل آمده درخصوص طبقه بندی جرائم رایانه‌ای می پردازیم و سپس با تجزیه و تحلیل آنها و ارائه یک طبقه بندی نظری به این بحث خاتمه می‌دهیم.

در پایان نامه‌ها و مقالاتی که درسا ل‌های اخیر در خصوص جرائم رایانه‌ای نوشته شده است، اولین اقدامات انجام شده درخصوص طبقه بندی جرائم رایانه‌ای را اقدامات اولیه سازمانهایی مانند (OECD)، شورای اروپا، انجمن بین المللی حقوق جزا و سازمان ملل متحد می‌دانند. در حالی که اقدامات اولیه این سازمانها صرفاً اقدامی در جهت تعیین مصادیق جرائم رایانه‌ای بوده است. اقدامات اولیه این سازمانها در زمانی صورت گرفته است که بسیاری از کشورها در تعیین مصادیق جرم رایانه‌ای با هم اختلاف نظر فاحش داشته‌اند. بنابراین اقدامات انجام شده اولیه را نمی‌توان اقدامی در جهت طبقه بندی جرائم رایانه‌ای محسوب کرد. اقدامات مذکور کوششی در جهت تعیین مصادیق جرم رایانه‌ای بوده اند. اکنون از به بررسی اقدامات سازمانهای بین المللی در زمینه طبقه‌بندی جرائم می‌پردازیم.

الف: طبقه بندی جرائم رایانه‌ای توسط سازمان های بین الملل

۱) اقدامات OECD

سازمان همکاری و توسعه اقتصادی (OECD) اولین سازمان بین المللی است که در سال ۱۹۸۳ به مطالعه و بررسی مسئله جرم یا سوء استفاده‌های رایانه‌ای پرداخت. این سازمان در سال ۱۹۸۶ گزارشی تحت عنوان جرم رایانه‌ای و تحلیل سیاستهای قانونی منتشر ساخت. در این گزارش ضمن ارائه تعریفی از سو ء استفاده‌های رایانه‌ای فهرستی به عنوان حد اقل سوء استفاده های رایانه‌ای که می‌تواند جرم تلقی شوند، ارائه داد و از کشورها خواست که با استفاده از قوانین کیفری آنها را مشمول ممنوعیت و مجازات قرار دهند. گزارش OECD را نمی‌توان اقدامی در جهت طبقه بندی جرائم رایانه‌ای به حساب آورد. این گزارش پنج نوع از اعمالی را که قابلیت جرم انگاری تحت عنوان جرم رایانه‌ای دارند، به تفکیک ذکر کرده است. این اعمال عبارتند از:

۱–ورود، تغییر، پاک‌کردن و یا متوقف سازی داده‌ها و یا برنامه‌های رایانه‌ای که به طور عمدی و با قصد انتقال غیر قانونی وجوه و یا هر چیز با ارزش دیگر صورت گرفته باشد.

۲–ورود، تغییر، پاک کردن و یا متوقف‌سازی داده‌ها و یا برنامه‌های رایانه‌ای که به طور عمدی و با قصد ارتکاب جعل صورت گرفته باشد.

۳–ورود ،تغییر، پاک کردن ویا متوقف سازی داده‌ها و یا برنامه‌های رایانه‌ای که به طور عمدی و با قصد جلو گیری از عملکرد سیستم رایانه‌ای و مخابراتی صورت گرفته باشد.

۴–تجاوز به حقوق انحصاری مالک یک برنامه رایانه‌ای حمایت شده با قصد بهره برداری تجاری از آن برنامه‌ها و ارائه آن به بازار.

۵–دستیابی یا شنود در یک سیستم رایانه‌ای و یا ارتباطی که آگاهانه و بدون کسب مجوز از افراد مسئول سیستم مزبور چه با تخطی از تدابیر امنیتی وچه با هدف غیر شرافتمندانه صورت گرفته باشد.

۲) اقدامات شورای اروپا

شورای اروپا درسال ۱۹۸۹ در توصیه نامه R(۸۹) دو فهرست تحت عنوان فهرست حداقل و فهرست اختیاری جرائم رایانه‌ای ارائه داد. جرائم فهرست حداقل عبارتند از:

۱–کلاهبرداری رایانه‌ای

۲–جعل رایانه‌ای

۳–وارد کردن خسارت به داده‌ها یا برنامه های رایانه‌ای

۴–خرابکاری رایانه‌ای (سابوتاژ)

۵–دستیابی غیر مجاز رایانه‌ای

۶–شنود غیر مجاز رایانه‌ای

۷– تکثیر غیر مجاز برنامه حمایت شده رایانه‌ای

۸–تکثیر غیر مجاز یک توپوگرافی

جرائم فهرست اختیاری عبارتند از :

۱–تغییر داده‌ها یا برنامه های رایانه‌ای

۲–جاسوسی رایانه‌ای

۳–استفاده غیر مجاز از رایانه

۴–استفاده غیر مجاز از یک برنامه حمایت شده رایانه‌ای

همانطور که ملاحظه شد توصیه نامه R(۸۹) شورای اروپا نیز همانند گزارش (OECD) اقدامی در جهت معرفی اعمالی است،که قابلیت جرم انگاری تحت عنوان جرائم رایانه‌ای را دارند و به هیچ وجه اقدامی در جهت طبقه بندی جرائم رایانه‌ای محسوب نمی‌شود.

۳)قدامات انجمن بین‌المللی حقوق جزا

انجمن بین‌المللی حقوق جزا نیز در نشست سال ۱۹۹۲ خود در ورتسبورگ آلمان بدون اینکه اقدامی در جهت طبقه بندی جرائم رایانه‌ای به عمل آورد، فهرست های حداقل و اختیاری شورای اروپا را به عنوان مصادیق پذیرفته شده جرم رایانه‌ای تأیید کرد.و در نشست ۱۹۹۴ خود در ریودوژانیرو ضمن تأکید مجدد بر فهرستهای مزبور از جرائم زیر به عنوان جرم رایانه‌ای نام برد:

۱-قاچاق کلمات رمز

۲-انتشار ویروس یا برنامه های مشابه

۳-دستیابی به اسرار بر خلاف قانون

۴-به کار گیری، انتقال ودگرگونی داده‌های شخصی[۵۶]

٤)طبقه بندی سازمان ملل متحد:

سازمان ملل متحد اولین سازمانی است که اقدامی هر چند کوچک در جهت طبقه بندی جرائم رایانه‌ای به عمل آورده است. این سازمان در نشریه بین المللی سیاست جنایی خود (شماره های ۴۳و۴۴) جرائم رایانه‌ای را به دو دسته به شرح زیر تقسیم کرده است:

«جرائم رایانه‌ای می‌تواند شامل فعالیتهای مجرمانه‌ای باشد که ماهیتی سنتی دارند از جمله سرقت،کلاهبرداری، جعل و سوءاستفاده که همگی معمولا در همه جا مشمول ضمانت اجراهای کیفری می شوند. رایانه نیز راههای تازه‌ای را برای سوء استفاده پدیدآورده است که می توانند ویا باید مجرمانه محسوب شوند.»

در این نشریه بر اقدامات شورای اروپا و (OECD) مبنی بر احصاء مصادیقی از جرائم رایانه‌ای تأکید شده است. سپس تعدادی از جرائم رایانه‌ای را به عنوان جرائم مشترک و عمومی یعنی جرائمی که جرم بودن آنها از نظر عموم کشورها پذیرفته شده است، احصاءکرده است و تعدادی از اعمال دیگر که مجرمانه بودن آنها هنوز از جانب عموم کشورها پذیرفته نشده ولی مشکلاتی را برای حقوق خصوصی و فردی ایجاد کرده‌اند، ذکر کرده است.

انواع مشترک وعمومی جرائم رایانه‌ای از دید سازمان ملل به شرح زیر است:

۱-کلاهبرداری رایانه‌ای

۲-جعل رایانه‌ای

۳-ایجاد خسارت (تخریب) یا تغییرداده‌ها و برنامه‌های رایانه‌ای

۴-دستیابی غیر مجاز به سیستمها وخدمات رایانه‌ای

۵-تکثیر غیر مجاز برنامه های رایانه‌ای حمایت شده

۵) طبقه بندی اینترپول (سازمان پلیس جنایی بین المللی):

سازمان پلیس جنایی بین المللی (اینترپول) به عنوان یک سازمان اجرایی بین المللی که سال ها است در زمینه مبارزه با جرائم رایانه‌ای فعالیت می کند،جرائم رایانه‌ای رابه شرح زیر طبقه بندی کرده است.

۱-دستیابی غیر مجاز که خود شامل سه جرم مستقل به شرح زیر است:

۱-۱-نفوذ غیر مجاز (هک)

۵۶- نشریه بین المللی سیاست جنایی،ش۴۳و۴۴ جرائم کامپیوتری جلد یک،شورای عالی انفور ماتیک،۱۳۷۶،ص۴۸

۲-۱-شنود غیر مجاز
۳-۱-سرقت زمان رایانه
۲-تغییر داده‌های رایانه‌ای که خود شامل چهار جرم به شرح زیر است:
۲-۱-تغییرداده‌ها لز طریق بمب منطقی
۲-۲-تغییرداده‌ها از طریق اسب تروا
۲-۳-تغییرداده‌ها از طریق ویروس رایانه
۲-۴-تغییر داده‌ها از طریق کرم رایانه‌ای
۳-کلاهبرداری رایانه‌ای که خود شامل شش جرم به شرح زیر است:
۳-۱-سوء استفاده از صندوق های پرداخت اتوماتیک پول(AIM)
۳-۲-جعل رایانه‌ای
۳-۳-سوء استفاده از ماشینهای بازی
۳-۴- دستکاری در مرحله ورودی خروجی
۳-۵-سوء استفاده از ابزار پرداخت مستقر در فروشگاهها
۳-۶-سوء استفاده تلفنی (به منظور استراق سمع یا استفاده از خدمات مخابرات)
۴-تکثیر غیر مجاز که خود شامل سه جرم زیر است:
۴-۱-تکثیر بازیهای رایانه‌ای
۴-۲-تکثیر توپو گرافی (نیمه هادی)
۴-۳-تکثیر نرم افزار های دیگر
۵-خرابکاری رایانه‌ای (سابوتاژ) که خود شامل دو جرم به شرح زبر است:
۵-۱-خراب کردن سخت افزار
۵-۲- خراب کردن نرم افزار
۶-سایر جرائم رایانه‌ای که شامل:
۶-۱-سرقت اسرار تجاری (افشاء انتقال واستفاده)
۶-۲-ذخیره سازی پورنوگرافی کودک وسایر نرم افزارهای غیر قانونی
۶-۳-سایر موضوعات قابل تعقیب[۵۷]

۶) طبقه بندی کنوانسیون بوداپست

کنوانسیون بوداپست یکی از اسناد بین المللی می باشد که در سال ۲۰۰۱ به امضای ۳۰ کشور جهان رسیده است.

۵۷- پرویزی، رضا، همان،ص۲۴-۳۲

بخش اول از فصل دوم این کنوانسیون شامل مقررات مربوط به جرم انگاری وسایر شرایط مربوط به جرائم رایانه‌ای یا جرائم مربوط به رایانه است.در این بخش ۹ جرم در چهار طبقه مختلف گروه بندی گردیده و هر یک از این جرائم بطور مجزا تعریف شده‌اند.

چهار طبقه مختلف جرائم رایانه‌ای مقرر در این کنوانسیون عبارتند از:

طبقه اول :جرائم علیه محرمانگی،تمامیت ودر دسترس بودن داده‌ها وسیستمهای رایانه‌ای.

جرائمی که زیر مجموعه این طبقه قرار دارند عبارتند از:

۱-دستیابی عمدی ومن غیر حق به سیستم رایانه‌ای

۲-شنود عمدی ومن غیر حق داده‌های رایانه‌ای

۳-ایجاداختلال عمدی ومن غیر حق در داده‌های رایانه‌ای

۴-ایجاد اختلال عمدی ومن غیر حق در سیستم رایانه‌ای

۵-سوء استفاده از وسایل،رمز عبور،کد دستیابی یا داده‌ها یا برنامه‌های رایانه‌ای

طبقه دوم:جرائم مرتبط با رایانه.جرائمی که زیر مجموعه این طبقه قرار دارند عبارتند از:

۱-جعل مرتبط با رایانه

۲-کلاهبرداری مرتبط با رایانه

طبقه سوم:جرائم مرتبط با محتوی.جرائمی که زیر مجموعه اینن طبقه قرار دارند عبارتند از:

۱-تولید هرزه نگاری (پورنوگرافی) کودکان به قصد انتشار درسیستم رایانه

۲-عرضه هرزه نگاری کودکان از طریق سیستم رایانه

۳-توزیع هرزه نگاری (پورنوگرافی) کودکان به قصد انتشار درسیستم رایانه

۴-تهیه هرزه نگاری (پورنوگرافی) کودکان به قصد انتشار درسیستم رایانه

۵-در اختیار داشتن هرزه نگاری (پورنوگرافی) کودکان به قصد انتشار درسیستم رایانه

طبقه چهارم:جرائم مرتبط با نقض مالکیت معنوی (کپی رایت).این طبقه ازجرائم نیزدارای مصادیقی است که هر کدام جرم مستقلی محسوب می شوند.

ب: طبقه بندی نظری جرائم رایانه‌ای

همانطور که در نشریه بین المللی سیاست جنایی سازمان ملل اشاره شده است،رایانه علاوه بر انکه راههای تازه ای برای سوء استفاده به وجودآورده که باید جرم انگاری شوند،وسیله وابزاری برای ارتکاب جرائمی که ماهیت سنتی دارند نیز می باشد.

بنابراین بطور کلی جرائم رایانه‌ای را می‌توان به دو دسته تقسیم کرد:

۱-جرائم رایانه‌ای سنتی.

۲-جرائم رایانه‌ای مدرن.

هر یک از جرائم رایانه‌ای سنتی و مدرن را بطور مختصر می‌توان اینگونه تعریف کرد:

جرائم رایانه‌ای سنتی جرائمی هستند که با همان شرایط قانونی که از طرق مرسوم ارتکاب می‌یابند، بوسیله رایانه نیز ارتکاب می‌یابند و قانونگذار ارتکاب بوسیله رایانه را به عنوان جزئی از اجزاء عنصر مادی آنها یا عامل تشدید و یا تخفیف مجازات آنها ذکر نکرده باشد.

جرائم رایانه‌ای مدرن جرائمی هستند که غالباً پس از پیدایش رایانه بوجود آمده‌اند و با پیشرفت رایانه تحول پیدا کرده‌اند و به موجب قانون رایانه به عنوان موضوع و یا ابزار جرم وجزئی از اجزاء تشکیل دهنده عنصر مادی آنها را تشکیل می دهد.

جرائم رایانه‌ای سنتی را می توان به پنج دسته به شرح زیر تقسیم کرد:

۱–جرائم رایانه‌ای علیه اشخاص

۲–جرائم رایانه‌ای علیه اموال

۳–جرائم رایانه‌ای علیه آسایش و امنیت عمومی

۴–جرائم رایانه‌ای علیه عصمت و عفت و اخلاق حسنه

۵–جرائم رایانه‌ای علیه خانواده

جرائم رایانه‌ای مدرن را نیز می توان به شش دسته به شرح زیر تقسیم کرد:

۱–جرائم رایانه علیه محرمانگی، تمامیت و در دسترس بودن داده‌ها مانند دستیابی غیر مجاز، شنود غیرمجاز،اختلال در داده

۲–جرائم رایانه‌ای علیه سیستم رایانه‌ای مانند اختلال در سیستم

۳–جرائم رایانه‌ای علیه اموال مانند کلاهبرداری رایانه‌ای

۴–جرائم رایانه‌ای علیه امنیت و آسایش عمومی مانند جعل رایانه‌ای

۵–جرائم رایانه‌ای علیه مالکیت معنوی

۶–جرائم رایانه‌ای علیه محتوی مانند انتشار پورنوگرافی کودک

آنچه که مبنا و محور تقسیم بندی نظری قرار گرفته است، ارزشهایی هستند که مورد حمایت قانونگذار بوده و مورد تجاوز و تعدی مجرمین قرار گرفته‌اند. جرایم رایانه‌ای را از جهات دیگر نیز طبقه‌بندی کرده‌اند که به لحاظ رعایت اختصار از ذکر آنها خودداری می‌شود.

نتیجه گیری

همانگونه که حقوقدانان کشورهای مختلف و متخصصان حقوق کیفری اطلاعات درسازمانهای بین‌المللی گفته‌اند نمی‌توان تعریفی از جرم رایانه‌ای ارائه کرد که در همه نظامهای حقوقی مورد قبول واقع شده و از نظر حقوقدانان و سایر افرادی که به هر نحو با حقوق کیفری اطلاعات سر وکار دارند فاقد ایراد و اشکال بوده و در همه زمینه های تئوری و عملی قابل استفاده باشد. بنابراین از سه دیدگاه مختلف می توان جرایم رایانه‌ای را تعریف کرد.

۱- گروهی که از دیدگاه قانونگذاری و جرم انگاری به پدیده جرم رایانه‌ای می‌نگرند، جرم رایانه‌ای را صرفا شامل آن دسته از جرائمی می‌دانند که بعد از پیدایش رایانه بوجود آمده‌اند (جرائم مدرن رایانه‌ای یا جرائم رایانه‌ای محض). هدف این گروه شناسایی این جرائم و مبارزه با آنها از طریق جرم انگاری و سایر تدابیر پیشگیرانه است.از این دیدگاه جرم رایانه‌ای رامی‌توان به شرح زیرتعریف کرد:

هرجرمی که به موجب حکم صریح قانون سیستم و یا داده رایانه‌ای به عنوان موضوع و یا وسیله آن اعلام شده و در نتیجه جزء عنصرمادی آن باشند، جرم رایانه‌ای نامیده می‌شود.

۲- گروهی دیگر که از دیدگاه جرم شناسی به پدیده جرم رایانه‌ای می‌نگرند، علاوه بر جرائم رایانه‌ای محض آن دسته از جرائم سنتی را نیز که بدون تغییر ماهیت بوسیله رایانه ارتکاب می‌یابند و مشمول قوانین قدیمی هستند از مصادیق جرم رایانه‌ای می‌دانند.

این گروه با دید وسیعتری به جرم رایانه‌ای می‌نگرند. از این دید گاه تعریف جرم رایانه‌ای به شرح زیر است:

هر جرمی که سیستم یا داده رایانه‌ای عملاً موضوع و یا وسیله ارتکاب آن باشد، اعم از این که قانونگذار رایانه رابه عنوان وسیله ارتکاب آن اعلام کرده یا نکرده باشد، جرم رایانه‌ای نامیده می‌شود.

۳- گروه سوم که از دیدگاه آئین دادرسی کیفری به جرم رایانه‌ای می‌نگرند، تعریف بسیار موسعی را برای جرم رایانه‌ای ارائه داده‌اند که از دو تعریف قبلی وسیعتر است. از این دید گاه تعریف جرم رایانه‌ای به شرح زیر است:

هر جرمی که رایانه به نحوی به عنوان موضوع یا ابزار جرم در آن نقش داشته باشد و یا دلایل یا اطلاعات مربوط به آن در رایانه ذخیره یا پردازش یا منتقل شده باشد،جرم رایانه‌ای نامیده می شود.

شورای اروپا با این دیدگاه در بند ۳۰ گزارش توجیهی توصیه نامه R(۹۵) به جای جرم رایانه‌ای از اصطلاح جرم فناوری اطلاعات استفاده کرده و آن را شامل آن دسته از جرائم که اطلاعات راجع به آنها در رایانه پردازش یا منتقل شده باشد، نیز می‌داند.

در خصوص طبقه‌بندی جرایم رایانه‌ای نیز همانطور که ملاحظه شد کنوانسون جرائم سایبر کاملترین وعلمی ترین کوشش واقدام بین‌المللی است که تاکنون در زمینه طبقه‌بندی جرائم رایانه‌ای به عمل آمده است. البته مصادیق جرم رایانه‌ای شناخته شده بسیار فراتر وگسترده تر از اعمال مجرمانه ای است که در کنوانسیون جرائم سایبر احصاء و تعریف شده اند.در بند۳۴ گزارش توجیهی کنوانسیون مزبور نیز به این نکته تصریح شده است که «جرائم مندرج در این کنوانسیون نشانگر یک توافق حداقل است که از بسط و توسعه آن در حقوق داخلی ممانعت نمی کند.»

فعالیت‌های سازمان‌های بین‌المللی جهانی و منطقه ای و سایر کوششهای بین‌المللی که تاکنون در خصوص جرائم بین‌المللی به عمل آمده است بیشتر ناظر بر جرم انگاری راههای تازه سوء استفاده است که بعد از پیدایش رایانه به وجودآمده اند.سازمانهای بین‌المللی کمتر به جرائم سنتی که به وسیله رایانه ارتکاب می یابند وخود بخود مشمول ضمانت اجرای کیفری می‌شوند پرداخته‌اند. در تفسیم بندی که کنوانسیون جرائم سایبرمصوب ۲۰۰۱ بوداپست جرائم رایانه‌ای به عمل آورده جایگاه جرائم سنتی رایانه‌ای مشحص نشده است. با توجه به نفوذ عمیق رایانه در تمام عرصه ها و ابعاد زندگی انسان بسیاری از جرائم سنتی قابلیت ار تکاب به وسیله رایانه را دارند.

امروزه قتل عمد و قتل غیر عمد ایراد صدمه بدنی اعم از عمد و غیر عمد که از مهمترین مصادیق جرائم علیه اشخاص هستند می‌توانند از طریق دستیابی به سیستم رایانه‌ای بیمارستانها ارتکاب یابند. توهین و افترا و نشر اکاذیب که از جرائم علیه شخصیت معنوی اشخاص محسوب می شوند، می‌توانند در مقیاسی بسیار گسترده تر از گذشته از طریق رایانه ارتکاب یابند.همچنین بسیاری از جرائم علیه اموال مانند اختلاس و آن دسته از کلاهبرداری ها که فردی از طریق رایانه دیگری را می فریبد و اموال او را می برد و یا تخریب از طریق اختلال در برنامه حرکت وسایل نقلیه زمینی و هوایی می توانند از طریق رایانه ارتکاب یابند.

علاوه بر جرائم علیه اموال و اشخاص بسیاری از جرائم علیه آسایش و امنیت عمومی مانند جعل اسکناس وسایر اوراق بهادار، جعل اسناد رسمی، جاسوسی، تبلیغ علیه نظام، اهانت به مقدسات، تروریسم سایبر (رایانه‌ای) و جرائم علیه عصمت و عفت و اخلاق حسنه مانند تشویق به فساد، سکس سایبر، ایجاد و توزیع و عرضه انواع صور قبیحه ومستهجن (هرزه نگاری) و بسیار آسانتر از گذشته و در مقیاس بسیار گسترده‌تر از قبل به وسیله رایانه انجام می‌شوند. مرتکب اینگونه جرائم بدون اینکه نیاز به قانونگذاری جدید باشد به موجب قوانین سنتی قابل مجازات است.

به نظر می‌رسدکه آن دسته از جرائم سنتی که علی‌رغم ارتکاب به وسیله رایانه به لحاظ حفظ ماهیت خود نیاز به جرم انگاری جدید ندارند، جزء جرائم رایانه‌ای هستند و باید آنها را در طبقه‌بندی جرائم رایانه‌ای لحاظ کرد.

☑ **عنوان: اقدامات سازمانهای بین المللی و منطقه‌ای در خصوص جرایم رایانه‌ای**

☑ **نویسنده: دکتر بتول پاکزاد**

(دانشجوی دکتری حقوق جزا و جرم شناسی دانشگاه شهید بهشتی و عضو هیئت علمی دانشگاه)

مقدمه

فناوری اطلاعات یکی از بزرگترین دستاوردهای علوم بشری است. این فناوری حیات را در کره خاکی به گونه‌ای دگرگون ساخته است که سایر فناوری‌های به وجود آمده در طول تاریخ بشر، در انجام آن ناتوان مانده‌اند.

فناوری اطلاعات تأثیر عمیقی بر اقتصاد، ارتباطات، فرهنگ، آموزش و تعامل اجتماعی کلیه کشورها گذاشته، آن‌ها را به دهکده جهانی نزدیک‌تر کرده و پایه‌های تمدن جدید بشر را بنا نهاده است.

از بدو پیدایش و همزمان با توسعه این تکنولوژی سوء استفاده از آن توسط مجرمان آغاز و توسعه یافته است به نحویکه امروزه اشکال متنوع جرایم مرتبط با رایانه و تکنولوژی اطلاعات تهدید جدی نه تنها نسبت به منافع افراد و منافع کشورها است و بلکه با توجه به بین‌المللی بودن این تکنولوژی علیه جامعه بین‌المللی است.

همین امر موجب واکنش سازمانهای بین‌المللی و منطقه‌ای نسبت به این جرایم گردیده است و پیش‌گیری و مبارزه با این جرایم که غالباً بعد فراملی دارد و بعضاً شکل سازمان یافته نیز به خود گرفته است مستلزم اقدامات هماهنگ در سطح ملی و بین‌المللی است. بدین منظور سازمانهای فوق در راستای هماهنگی قوانین و مقررات داخلی در زمینه‌های حقوق جزای ماهوی، آیین دادرسی و جزای بین‌المللی سعی در ارائه رهنمودها و توصیه‌های مقتضی به کشورهای عضو نموده‌اند.

بررسی این اقدامات از جهات مختلف بویژه انعکاس در حقوق داخلی و هماهنگی با سایر کشورها در راستای مبارزه مؤثر با این جرایم و پیش‌گیری از آنها مفید بنظر می‌رسد.

۱- اقدامات سازمان توسعه و همکاری اقتصادی (OECD)[۱]

سازمان توسعه و همکاری اقتصادی (OECD) نخستین تلاشهای گسترده را در مورد مشکلات حقوق کیفری در باب جرایم رایانه‌ای را آغاز نمود. سال ۱۹۸۳ تا ۱۹۸۵ یک کمیته اختصاصی OECD مشغول مطالعه و بررسی راههای ممکن جهت هماهنگی بین‌المللی قوانین کیفری برای مبارزه با جرائم اقتصادی مرتبط با رایانه شد.

۱- Organisation for Electronic cooperation and Development

سازمان همکاری و توسعه اقتصادی در ۲۱ دسامبر ۱۹۵۹ با امضای اعلامیه مشترک که رؤسای دولتهای فرانسه ـ ایالات متحده امریکا ـ جمهوری فدرال آلمان و بریتانیا امضاء نمودند و با اهداف توسعه کشورهای توسعه نیافته و توسعه روابط بازرگانی بین‌المللی ایجاد شد. در حال حاضر این سازمان متشکل از مهمترین کشورهای دارای اقتصاد آزاد است و کانادا ـ ژاپن و استرالیا و زلاند جدید علاوه بر کشورهای اروپایی عضو، دیگر اعضای این سازمان هستند.

این کمیته برای ارائه گزارش خود ابتدا پرسش‌نامه‌های مفصلی به دول عضو آن سازمان فرستاد که در آن خطوط اصلی سیاست قضائی در واکنش نسبت به جرائم رایانه‌ای، بررسی قابلیت اجرا یاعدم قابلیت اجرای حقوق کیفری و یکسری اطلاعات دیگر ذکر شده بود.

در سال ۱۹۸۶ گزارشی تحت عنوان جرم رایانه‌ای تحلیل سیاست‌های قضائی منتشر ساخت که به بررسی قوانین موجود و پیشنهادهای اصلاحی چند کشور عضو می‌پردازد و براساس تجزیه و تحلیل تطبیقی قوانین ماهوی، پیشنهاد کرد فهرست اقدامات زیر می‌تواند به عنوان خطوط مشترکی در روش‌های متفاوت اتخاذ شده از سوی کشورهای عضو در نظر گرفته شده و مشمول ممنوعیت و مجازات قرار گیرند.

۱-۱- تبیین انواع جرائم رایانه‌ای

OECD جرم رایانه‌ای را چنین تعریف می‌کند: « سوء استفاده از رایانه شامل هر رفتار غیرقانونی، غیراخلاقی یا غیرمجاز مربوط به پردازش اتوماتیک و انتقال داده‌هاست.» رهیافت موسع و تکنیکی در این تعریف آشکار است. فهرست حداقل سوء استفاده هایی که باید مشمول ممنوعیت و مجازات قرار گیرند از سوی OECD که به عنوان اولین تقسیم‌بندی جرائم رایانه‌ای نیز حائز اهمیت می‌باشد، و شامل موارد زیر است:

الف) ورود، تغییر، پاک کردن و یا موقوف‌سازی داده‌های رایانه‌ای و یا برنامه‌های رایانه‌ای که به طور ارادی و با قصد انتقال غیرقانونی وجوه یا هرچیز باارزش دیگر صورت گرفته باشد.

ب) ورود، تغییر، پاک کردن و یا موقوف‌سازی داده‌های رایانه‌ای و یا برنامه‌های رایانه‌ای که به صورت عمدی و یا قصد ارتکاب جعل صورت گرفته باشد.

ج) ورود، تغییر، پاک کردن و یا موقوف‌سازی داده‌های رایانه‌ای و یا برنامه‌های رایانه‌ای یا هرگونه مداخله دیگر در سیستم‌های رایانه‌ای، که به صورت عمدی و با قصد جلوگیری از عملکرد سیستم رایانه‌ای و یا ارتباطات صورت گرفته باشد.

د) تجاوز به حقوق انحصاری مالکیت یک برنامه رایانه‌ای حفاظت شده با قصد بهره‌برداری تجاری از آن برنامه و ارائه آن به بازار

ه) دستیابی یا استراق سمع در یک سیستم رایانه‌ای و یا ارتباطی که آگاهانه و بدون کسب مجوز از فرد مسئول سیستم مزبور چه با تخطی از تدابیر امنیتی و چه با هدف غیرشرافتمندانه و یا مضر صورت گرفته باشد.

نکته مهم در این لیست رهیافت فنی صرف تدوین‌کنندگان آن است که نمی‌توانست حقوقدانان و متخصصان مربوطه را در رویارویی صحیح و بموقع در برابر اشکال متنوع جرایم رایانه‌ای یاری دهد و بناچار می بایست اقدامات بعدی جهت اصلاح یا تغییر یا تکمیل لیست صورت می‌گرفت.

۲-۱- سایرمشکلات ناشی از جرایم رایانه‌ای

گزارش OECD در سال ۱۹۸۶ بطور عمده موضوعات حقوق جزای ماهوی را در رابطه با جرایم رایانه‌ای مورد بررسی قرارداد و فقط به تعداد محدودی از موضوعات آئین دادرسی کیفری پرداخت.

در فصل ۴ در جنبه‌های بین‌المللی در رابطه با **صلاحیت** توصیه کرد که « این موضوع مورد رسیدگی قرار گیرد که چگونه در سطح بین‌المللی، سرکوب وجلوگیری جرائم مربوط به رایانه در موقعیت‌هایی که دو یا تعداد بیشتری از کشورها صلاحیت

تعقیب یک جرم رایانه‌ای را دارند، هماهنگ شود.» گزارش همچنین موضوع قابلیت اعمال اصول و اسناد بین‌المللی از قبیل **استرداد و معاضدت متقابل قضایی** در خصوص جرایم مربوط به رایانه را ذکر کرد.

گزارش OECD همچنین مشکلات دیگری از قبیل ادله، ضمانت اجراها، اجرای حکم‌های خارجی به خاطر پیشگیری و مبارزه با جنبه‌های فراملی جرم رایانه‌ای مستلزم توجه بیشتری دانست و نهایتاً به مسئله «**تفتیش شبکه فرامرزی**» به طور مختصر اشاره می‌کند.

در گزارش ۱۹۸۷ یک فصل جامع به تعقیب بین‌المللی جرایم رایانه‌ای اختصاص یافته است و در قسمت نتیجه‌گیری جستجوی «شبکه فرامرزی» را به عنوان یکی از بنیادی‌ترین ابزار تحقیقات جنایی در رابطه با جرایم مربوط به رایانه معرفی کرد و صریحاً پیشنهاد کرد که در همکاری با شورای اروپا اقداماتی را آغاز کند که یک رویه فوری را در خصوص اعمال نیابت قضائی تسهیل کند و آن دولتها را تحریک کند تا کاربرد اختیارات اجباری را در همان حدی که قانون ملی مقرر کرده است، در دسترس دولت‌های متقاضی قرار دهد. این گزارش همچنین پیشنهاد کرد که مطالعات راجع به مجاز بودن تفتیش فرامرزی داده‌ها در شبکه‌هایی رایانه‌ای به کمک شورای اروپا مورد حمایت ونظارت قرار گیرد ."

۲ – اقدامات شورای اروپا[۲]

پس از ارائه گزارش OECD ، شورای اروپا به دلایل چند ضرورت تدوین و پیگیری مطالب منعکس در گزارش را احساس کرد از جمله کلیت کار OECD ، ابهام در تقسیم‌بندی جرایم، عدم ارائه راه حل روشن و قانونی، عدم توجه به مشکلات یا ساختارهای سیستماتیک کشورهای عضو شورای اروپا و..... و همچنین با توجه به مسئله آزادی‌های مدنی، حقوق فردی و نیاز به حمایت قانونی، این مسائل را از دیدگاه فنی حقوقی جهت ارائه رهنمودهایی به قانونگذاران، برای تعیین اینکه چه رفتارهایی باید براساس حقوق کیفری ممنوع شوند و روش اعمال آن چگونه خواهد بود، مورد مطالعه قرار داد.

مسئله جرم رایانه‌ای درسال ۸۶– ۱۹۸۵ در برنامه کار کمیته اروپایی مشکلات ناشی از جرم قرار گرفت این کمیته خود کمیته‌ای تخصصی را برای مطالعه این موضوع ایجاد کرد. این کمیته (**کمیته متخب کارشناسان جرم رایانه‌ای**) کار خود را در سال ۱۹۸۵ میلادی آغاز کرد. مطالعات و تحقیقات انجام شده تاکنون منتهی به مصوبات مهم و قابل توجه شورای اروپا در این زمینه شده است از جمله توصیه نامه شماره ۹ (۸۹) R شورای اروپا در مورد جرم رایانه‌ای که شامل رهنمودهایی برای قانونگذاران ملی می‌شود. در ۱۳ سپتامبر ۱۹۸۹ از سوی هیأت وزرای شورای اروپا پذیرفته شد. توصیه‌نامه شماره (۹۵) R ناظر به مشکلات آئین دادرسی کیفری مرتبط با فناوری اطلاعات و اهم آنها کنوانسیون جرایم سایبر (۲۳/ سپتامبر ۲۰۰۱ بوداپست) می‌باشد که در ادامه مورد بررسی قرار می‌گیرند. همچنین لازم است به توصیه‌نامه شماره ۱۰(۸۵) R درباره اجرای کاربردی کنوانسیون اروپایی راجع به همکاری دو جانبه در زمینه‌های کیفری جهت تبادل نامه‌های نیابت قضائی در زمینه شنود ارتباطات مخابراتی و نیز توصیه‌نامه شماره ۱۵ (۸۷) R که نحوه استفاده از داده های شخصی در امور پلیسی را مقرر می‌دارد و حاوی رهنمودهایی برای دولت‌ها در مورد راه‌های برخورد با مسایل مربوط به جمع‌آوری، ذخیره‌سازی، به کارگیری و نقل و انتقال داده‌های شخص به وسیله پلیس می‌باشد. و نیز توصیه‌نامه شماره ۴ (۹۵) R مورد

۲– اساسنامه شورای اروپا در ۱۹۴۹ به امضاء رسید و در همان سال به اجرا درآمد. کمیته وزیران شورای اروپا رکنی است که صلاحیت دارد بنام شورای اروپا اقدام نماید.

حمایت از داده های شخصی در زمینه خدمات ارتباطات مخابراتی، و توصیه‌نامه ۱۰ (۸۴) R سوابق کیفری و اعاده حیثیت مجرمان (استراتسبورگ ۱۹۸۴) ، نیز اشاره نمود.

۱-۲- توصیه نامه ۸۹ (۹) R

کمیته منتخب کارشناسان جرم رایانه‌ای کار خود را از ۱۹۸۵ آغاز نمود و نهایتاً در ۱۹۸۹ در آخرین نشست خود، یک گزارش و یک توصیه‌نامه به کمیته اروپایی مشکلات ناشی از جرم ارائه کرد و این کمیته آن را بررسی و پس از تأئید به کمیته وزرای شورای اروپا فرستاد. این توصیه‌نامه پس از بررسی‌های کارشناسانه بوسیله کمیته وزرا پذیرفته و به کشورهای عضو تسلیم شده تابا توجه به خطوط کلی و رهنمودهای ارائه شده بویژه ۲ فهرست حداقل (اجباری) وحداکثر (اختیاری) قوانین لازم رادرسیستم داخلی خود تنظیم نمایند.

این توصیه‌نامه[۳] حاوی ۵ فصل و ۳ ضمیمه می‌باشد[۴]، در فصل اول ملاحظات کلی (از جمله مربوط به سیاست جنایی)، در فصل دوم خطوط راهنما برای قانونگذاران ملی (دو فهرست اجباری و اختیاری از جرائم رایانه‌ای) در فصل سوم مشکلات مربوط به آئین دادرسی، در فصل چهارم جنبه‌های بین‌المللی و در فصل پنجم دیگر جنبه‌های جرم رایانه‌ای ذکر شده است.

۱-۱-۲- مسائل کلی وملاحظات مربوط به سیاست جنایی

در خصوص مفهوم جرم رایانه‌ای، از هر دو اصطلاح «جرم رایانه‌ای[۵]» و «جرایم مربوط به رایانه[۶]» بهره جسته وتفاوتی بین این دو قائل نیست و از آنجا که هر کوششی برای تعریف جرم رایانه‌ای با نوعی نارسایی روبرو می‌شود تعریف مستقلی از آن ارائه نداد و این امر به قانونگذاران ملی واگذار شد تا با توجه به سیستم قضائی خود، در کنار رهنمودهای ارائه شده تعریفی ارائه نمایند که دو فهرست اجباری و اختیاری را در برداشته باشد .

در ملاحظات مربوط به سیاست جنایی با توجه به اینکه در کشورهای عضو شورای اروپا بیش از۱۰ سال بود که پدیده جرم رایانه‌ای مورد توجه قرار گرفته بود، این امر که حقوق کیفری داخلی چه واکنش‌های مناسبی را باید در قبال انواع جدید سوء استفاده از تکنولوژی رایانه از خود نشان دهد، مورد بررسی قرار گرفته است و با توجه به مشکلات تقریباً یکسان در همه کشورهای صنعتی درخصوص تعقیب و نحوه رسیدگی به این جرائم و نیز با توجه به اینکه این جرائم گاهی به صورت فرامرزی انجام می‌شوند و مشکلاتی از حیث تعاون بین‌المللی ایجاد شده است، نیاز به یک استراتژی مشترک احساس و سطوح مختلف زیر برای مبارزه با این جرایم در نظر گرفته شد:

- تعیین جرایم رایانه‌ای بوسیله اصلاح یا تکمیل قوانین کیفری ماهوی
- تعقیب موثر از طریق مقررات دادرسی کیفری متناسب
- ارتقای سطح همکاری بین‌المللی

۳- مأخذ: جرم رایانه‌ای، شورای اروپا، استراسپورگ ۱۹۹۰، ترجمه، جلد اول جرایم رایانه‌ای، دبیرخانه شورای عالی انفورماتیک

۴- ضمائم شامل فهرست اجباری و اختیاری، جرائم، کتاب‌شناسی است. جهت اطلاع بیشتر به مأخذ فوق مراجعه شود.

۵- Computer crime

۶- Computer related crime

کمیته محور مرکزی سیاست جنایی اروپا را نیز در این خصوص، بسط رهنمودهایی برای قانونگذاران ملی، با در نظر داشتن پیشرفتهای آینده در حقوق کیفری ماهوی قرار داده است. از آنجا که هماهنگ‌سازی سیستم‌های کیفری کار دشواری است کمیته به کنوانسیونی بین‌المللی به عنوان راه حل بعدی که باید بطور حتم ارائه شود عنایت کرده است . با اینحال سیاست جنایی اروپا با نگاهی به رهنمودها و نحوه جرم شناختن برخی اعمال در فصل (۲) مشخص می‌گردد.

منافعی که باید مورد حمایت کیفری قرار گیرند باید با توجه به اشکال مختلف سوء استفاده از سخت‌افزار، نرم‌افزار یا داده‌های رایانه‌ای یا حملاتی که به آنها می‌شود، درجه و توان خطرها و اجتناب از تورم کیفری تعیین گردند. همچنین تأکید شده است که علاوه بر مواردی که پردازش داده‌ها ورایانه به عنوان ابزار ارتکاب جرم استفاده شده است رایانه‌ای کردن امور منجربه موقعیتی شده که انواع جدیدی از منافع ایجاد شوند که نیازمند حمایت قضایی هستند از جمله صحت داده‌ها یا عملکرد سیستم رایانه‌ای این منافع جدید باید مورد حمایت حقوق کیفری قرار گیرند. زیرا در حقوق جزا تاکنون حمایت معطوف به موضوعات ملموس، عینی و فیزیکی بوده است البته این امر که حقوق جزا باید به عنوان آخرین راه حل در نظر گرفته شود، مورد توجه کمیته بوده است و یکی از بهترین تدابیر برای جلوگیری از ارتکاب جرم رایانه‌ای ارتقای تدابیر امنیتی و افزایش سطح آگاهیها نسبت به راههای احتمالی سوء استفاده توصیه شده است.

۲-۱-۲- خطوط راهنما برای قانونگذاران ملی

در فصل دوم توصیه‌نامه، با توجه به اینکه اعمال حقوق کیفری مرسوم نسبت به جرایم رایانه‌ای مشکلاتی را ایجاد می‌کند و از سوی دیگر مبارزه با این جرایم نیازمند سیاست جنایی متحدالشکل می‌باشد، رهنمودهایی را برای قانونگذاران کشورهای عضو ارائه نموده است. در این فصل رفتارهای خطرناک و مضر که باید جرم‌انگاری شود در دو فهرست ارائه شده‌اند. لیست حداقل یا اجباری که نشانگر اجماع و توافق اعضاء در مورد آنهاست و باید در حقوق کیفری کشورهای عضو جای گیرند و فهرست اختیاری که مبین عدم اجماع بر سر مفاهیم آن است و لذا چون برخی کشورها نقش اساسی برای این نوع جرایم قائلند و برخی خیر ونیز ازآنجاکه درآینده ممکن است این اشکال مجرمانه حالت جدی یابند ، دراین مقطع به صورت اختیاری ارائه شدند تا در صورت لزوم مورد تصویب قرار گیرند. جرم شناختن اعمال مذکور در فهرست اختیاری بستگی به ارزشها و ملاحظات در هر کشور دارد. قبل از بیان جرائم مذکور در هر فهرست لازم بذکراست ۱ـ علی‌رغم اینکه در تعریف هر یک از جرائم و نیز سایر مطالب از واژه‌های تخصصی چون داده‌ها، رایانه، یا سیستم رایانه‌ای استفاده شده است، اما از اصطلاحات تعریفی به عمل نیامده است و این امر ناشی از تصمیم کمیته برای اجتناب از مباحث بعدی بوده است زیرا اولاً تعاریف موجود جهت اهداف تکنیکی ارائه شده‌اند و در تفسیر قوانین کیفری نمی‌توانند بکار آیند. ۲ـ هر کشوری استاندار و تعریف‌های خاصی را مد نظر قرار داده است. با اینحال زیر هرعنوان مجرمانه ، یک متن تقسیری وتوضیحی نیز درج شده است که حاوی منافع مورد حمایت وعنای متشکله هرجرم می باشد. ۳ـ فقط جرایم عمدی مد نظر می‌باشند زیرا به عقیده کمیته رفتارهای توأم با بی‌مبالاتی و بی‌احتیاطی بطور اصولی نباید در جرایم رایانه‌ای مطرح باشد.

۱-۲-۱ فهرست حداقل یا اجباری

در فهرست حداقل جرائمی که ذکر شده‌اند از فهرست OECD فراتر رفته است و همچنین تفاوت بین انواع جرایم دقیق‌تر تبیین شده است و با توجه به تفاوت سیستم‌های کیفری کشورها، در رهنمودهای این فهرست اجماع لازم و کلی حاصل آمده

است و از هر گونه توسعه مفاهیم که با پیشینه حقوق ملی کشورهای عضو متضاد باشد اجتناب شده است و شامل ۸ عنوان مجرمانه بشرح ذیل می‌باشد:

الف) کلاهبرداری رایانه‌ای

«وارد کردن، تغییر، محو یا موقوف‌سازی داده‌های رایانه‌ای یا برنامه‌های رایانه‌ای یا دیگر مداخلات در پردازش داده‌ها که بر نتیجه پردازش‌ها اثر می‌گذارد و موجب ضررهای اقتصادی یا تصرف در اموال شخص دیگر به قصد تحصیل منفعت اقتصادی غیر قانونی برای خود یا دیگری می‌شود. (راه حل جایگزین: با قصد محروم کردن غیرقانونی آن شخص از اموالش) .»

ب) جعل رایانه‌ای

« وارد کردن، تغییر، محو یا موقوف‌سازی داده‌های رایانه‌ای یا برنامه‌های رایانه‌ای یا دیگر مداخلات در زمینه داده‌پردازی، از طریق یا تحت شرایطی که در قوانین ملی تشریح شده است، تشکیل دهنده جرم جعل است اگر به خاطر هدف‌های مرسوم چنین جرمی ارتکاب یافته باشد.»

ج) خسارت زدن به داده ها یابرنامه های رایانه‌ای (تخریب)

«محو، خسارت زدن، کم ارزش کردن یا موقوف سازی داده‌ها یا برنامه های رایانه‌ای بدون حق»

د) سابوتاژ رایانه‌ای

«واردکردن، تغییر، محو یا موقوف‌سازی داده‌ها یا برنامه‌های رایانه‌ای یا مداخله در سیستم‌های رایانه‌ای با قصد اختلال و جلوگیری از عملکرد رایانه یا سیستم ارتباطات.»

ه) دستیابی غیر مجاز

«دستیابی بدون حق به سیستم یا شبکه رایانه‌ای به وسیله تجاوز به تدابیر و ابزاهای امنیتی»

و) شنود غیرمجاز

«شنود که بدون حق بوسیله ابزارهای تکنیکی بر روی ارتباطات از طریق یا درحدود یک سیستم یا شبکه رایانه‌ای انجام شده است.»

ز) ارائه و ایجاد مجدد و غیرمجاز یک برنامه رایانه‌ای حمایت شده

« ایجاد مجدد، توزیع یا ارتباط با عامه، بدون حق از یک برنامه رایانه‌ای که بوسیله قانون حمایت شده است»

ح) ارائه و ایجاد مجدد یک توپوگرافی

«ایجاد مجدد بدون حق یک توپوگرافی از یک محصول نیمه‌های یا کشف تجاری یا مهم از این جهت که بوسیله قانون حمایت شده است و بدون حق انجام شود.»

۲-۲-۲۱-۲ – فهرست اختیاری

در ارائه فهرست اختیاری علاوه برعدم اجماع کشورهای عضو در جرم‌انگاری آنها این نکته مورد توجه بوده که اینگونه جرایم به طور معمول تا دیرباز از دید مقنن ملی هر کشور دور می‌ماند و لذا توجه به این جرائم لازم است. چهار عنوان مجرمانه در این فهرست مد نظر قرار گرفته‌اند:

الف) تغییر داده ها یا برنامه‌های رایانه‌ای

تغییر داده‌ها یا برنامه‌های رایانه‌ای بدون حق

ب) جاسوسی رایانه‌ای

بازرسی و تفتیش بوسیله ابزارهای لازم برای افشاء، انتقال یا استفاده از اسرار تجاری یا بازرگانی بدون داشتن حق یا بدون هیچ توجیه قانونی دیگری خواه با قصد ایجاد ضرر اقتصادی به شخص محق اسرار وخواه به قصد کسب یک منفعت اقتصادی غیرقانونی برای خود یا دیگری.

ج) استفاده غیرمجاز از رایانه

« استفاده از سیستم یاشبکه رایانه‌ای بدون حق که یا

۱- موجب خطر و صدمه به شخص محق در استفاده از سیستم شود یا صدمه به سیستم وارد آید یا عملکرد آن مشکل شود یا

۲- با قصد ایجاد ضرر برای شخص محق در استفاده از سیستم یا صدمه به سیستم یا عملکرد آن انجام شود، یا

۳- موجب ضرر به شخص محق در استفاده از سیستم یا صدمه به سیستم یا عملکرد آن شود.

د – استفاده غیرمجاز از برنامه‌های رایانه‌ای حمایت شده

«استفاده بدون حق از برنامه رایانه‌ای که بوسیله قانون حمایت شده و بدون حق مجدداً ایجاد شده است خواه به قصد تحصیل منفعت اقتصادی غیرقانونی برای خود یا دیگری، خواه به قصد ایجاد صدمه برای مالک (دارنده) حق.»

۳-۱-۲ – مشکلات مربوط به آئین دادرسی کیفری

فصل سوم توصیه‌نامه به مشکلات مربوط به آئین دادرسی کیفری از جنبه‌های مختلف اشاره دارد. و در مقدمه آن ذکر شده است که در همه کشورهای صنعتی تاکنون مباحثات قضائی مربوط به جرایم رایانه‌ای تنها به حقوق ماهوی متمرکز شده و از مسائل آئین دادرسی کیفری مربوط به این جرایم کوتاهی شده است. جنبه های دادرسی مختص رایانه نه تنها ازجهت تعقیب جرایم رایانه ای اهمیت دارد بلکه ازحیث تحقیقات جنای که لازم آن مراجعه به محیطهای رایانه‌ای شده است نیز با توجه به اینکه در اکثر یا همه جنبه‌های زندگی اجتماعی و اقتصادی، رایانه بکار گرفته شده است، اهمیت بیشتری داشته و نیزخواهد یافت. لذا مشکلات آئین دادرسی حول سه محورزیر مطرح شده اند:

الف) **قدرت‌های اجباری مقامات مجری قانون** برای کسب ادله در محیطهای رایانه‌ای شد، تحقیقات موفق در محیطهای رایانه‌ای شده مستلزم تخصص و مهارت لازم پلیسی و همکاری متخصصان و کاربران رایانه است مقررات موجود در آئین دادرسی در خصوص ورود و تفتیش اماکن، ضبط و توقیف ادله و ارائه ادله و.... مربوط به اموال مادی یا ارتباطات تلفنی بین انسانها می‌شود و اهداف غیرمادی و نیازهای جامعه اطلاعاتی رایانه‌ای را دربرنمی‌گیرد. در این قسمت مشکلات مربوط به موضوعات ذیل بررسی شده است:

- تفتیش و ضبط داده‌های ذخیره شده یا پردازش شده در سیستم داده‌پردازی
- وظایف همکاری فعال با مقام یا مأمور مجاز به تحقیق و ضبط و توقیف بدلیل اینکه داشتن اطلاعات کامل در باب سخت‌افزار، نرم‌افزار، سیستم‌های عملیاتی و .... برای مأمورین تحقیق همیشه امکان‌پذیر نیست.
- شنود سیستم‌های ارتباطات و ضبط داده‌ها یا اطلاعات ناشی سیستم‌های ارتباطات و رایانه‌ای قابلیت قبول و درجه تأثیر این ادله .

ب) قانونی بودن کسب، ذخیره‌سازی و استفاده از داده‌های شخصی در دادرسی‌های کیفری که بسته به نحوه حمایت در سیستم‌های قضائی کشورها دارد. اختیارات پلیس در این مورد باید به تفصیل مورد بحث قرار گیرد و در بعد بین‌المللی ابعاد وسیع‌تری نیز خواهد داشت.

ج) قابلیت قبول ادله بدست آمده از رایانه در رسیدگی‌های کیفری و مدنی است، اکثر کشورها ادله‌هایی را می‌پذیرند که مادی باشد اگر داده‌ها یا چاپگرهای رایانه‌ای خاص به عنوان دلیل نتواند استفاده شود نمی‌تواند مورد ضبط و تفتیش نیز واقع شود. ضمن اینکه داده‌ها و چاپگرهای فوق به راحتی قابل سوءاستفاده و تأثیر مستقیم بر قابلیت استرداد، معاضدت قضایی و.... دارد .

در این فصل صرفاً به طرح مشکلات آئین دادرسی پرداخته شده و رهنمودی ارائه نگردیده است زیرا شورای اروپا مشغول تدوین توصیه‌نامه‌ای مخصوص بود که بعداً منتشر شد. (توصیه‌نامه (۹۵) R که در مبحث بعد مورد بررسی قرار می‌گیرد.)

٤-۱-۲- جنبه‌های بین المللی

جرایم رایانه‌ای بلحاظ موقعیت فرامرزی که احراز کرده‌اند حائز اهمیت بسیار هستند، تکنولوژی جدید امکان ذخیره‌سازی، انتقال، استفاده از داده‌ها از طریق شبکه‌ها و ایجاد ارتباط و انتقال سریع درسطح وسیع بین سیستم‌های رایانه‌ای افزایش یافته است درنتیجه کشورها و محل‌های ذینفع در جرایم رایانه‌ای افزایش یافته‌اند. جرم ممکن است در چند کشور انجام شود یا از نقطه ای از دنیا کشور دیگری را دستخوش اعمال مجرمانه خود کنند. به عبارتی افراد مرتکب حضور فیزیکی در محل ندارند. همچنین شبکه‌های بین‌المللی داده‌ها نظر مجرمان را یک روزه به خود جلب کرده است. چون در این قضایا کاراکتر فرامرزی بودن مطرح است کمیته متوجه شد که اول عضو باید در قوانین مربوط به **تعیین محل ارتکاب** و **صلاحیت رسیدگی** و **تعقیب** تجدیدنظر به عمل آورند. همچنین باتوجه به سایرمشکلات ایجاد شده دراین محدوده به موارد ذیل پرداخته شده است :

الف) مشکلات صلاحیتی مربوط به خصیصه فرامرزی جرم رایانه‌ای

با توجه به خصیصه فرامرزی جرم رایانه‌ای چه ملاکی باید برای تعیین کشورصالح به رسیدگی چنین جرایمی به کار گرفت؟ جائی که مجرم حضور فیزیکی دارد یا جائی که بزهدیده یا ادله وجود دارد؟ تمایل بین‌المللی در بکارگیری این نظریه است که جائیکه یکی از عناصر جرم رخ داده است، یعنی حتی بخشی از یک جرم، صلاحیت رسیدگی دارد، که این امر منجربه تعارضات مثبت صلاحیتی می‌شود ولذا همکاری در تحقیق، تعقیب و مجازات جرائم ضروری بنظر می‌رسد البته برخی دولتها صلاحیت فراسرزمینی خود راعلاوه برخسارت‌هایی که به داده‌های حکومتی یا نظامی یا سابوتاژ رایانه‌ای که بر سیستم‌های مهم و بنیادی اثر می‌گذارد به منافع اقتصادی خود نیز توسعه داده‌اند. کمیته راه‌حل‌ها و مکانیسم‌های چند جانبه را برای کنترل تعارض صلاحیت‌ها پیشنهاد کرده است از جمله: هماهنگ ساختن تقنین‌ها، انتقال تشریفات رسیدگی و معاضدت متقابل در موضوعات کیفری. و برای روند یکپارچه‌سازی بین‌المللی فعلاً پیشنهاد می‌کند کنوانسیونی درخصوص جرایم رایانه‌ای تدوین و تصویب شود.

ب) مشکل دخالت مستقیم

گاه برای تحصیل دلیل از بین داده‌ها باید فراتر از حد مرزها تحقیقاتی بعمل آید و از آنجا که تکنولوژی نوین این امکان را بوجود آورده است که به طور حتمی به داده‌هایی در یک کشور دست یافت که در کشور دیگر ذخیره شده است، مسئله و مشکل مشروعیت دست‌یابی مستقیم (آن لاین) در دیگر دولت‌ها برای مقامات دولت تحقیق کنده پیرامون جرم است. در توصیه‌نامه

ضمن بررسی ابعاد این مشکل تأکید شده است که در فقدان یک توافق خاص بین دول مربوط، **مقامات تحقیق کننده مجاز به نفوذ و مداخله مستقیم نیستند** وباید از ابزارهای معاضدت قضائی بین‌المللی برای این کار کمک بگیرند و البته تحت برخی شرایط، مداخله مستقیم موجه قلمداد شده است:

– استفاده تنها برای اتخاذ تدابیری درخصوص حفظ وضع موجود است.

– داده‌ها استفاده نشوند مگر اینکه دولت مربوطه مجوز لازم را بدهد.

– ماهیت یاخطرناکی جرم، توجیه‌کننده مداخله باشد.

– ظن قوی باشد که زمان، اقتضای چنین عملی را دارد.

– مقامات تحقیق کننده ،مقامات کشور دیگر رامطلع سازند.

ج) قابلیت اعمال کنوانسیون های حقوق کیفری اروپا برای جرایم رایانه‌ای

– کنوانسیون اروپایی استرداد: شرایط اعمال کنوانسیون استرداد از جمله جرم بودن عمل در هر دو کشور و اینکه مجازات عمل ارتکابی حبس بیش ازیکسال باشد درخصوص جرایم رایانه‌ای، مستلزم یکپارچگی قوانین کیفری ماهوی است همچنین از حیث تعیین محل ارتکاب نیز دشواری وجود دارد.

– کنوانسیون اروپایی انتقال تشریفات رسیدگی در موضوعات جزایی، نکات فوق در اینجا نیز قابل ذکراست:

– کنوانسیون اروپایی معاضدت متقابل درموضوعات کیفری: از آنجا که ماده ۲ این کنوانسیون مقرر داشته اگر اجرای درخواست موجب صدمه به منافع دولت مورد تقاضا شده باشد، این امر ممکن است معاضدت متقابل رد شود، ممکن است منجر به محدودیت اجرای عملی کنوانسیون درجرایم رایانه‌ای شود، رسماً توصیه شده که زمینه‌های امتناع محدود به دو مورد زیر گردد:

۱– اگر مطابق قوانین دولت مورد تقاضا واقع شده، ماهیت یا شدت جرم، وضعیت شخصی که داده‌ها مربوط به اوست و یا آن را در تصرف دارد، مالک، مسئول سیستم رایانه‌ای، ماهیت خود داده‌ها که استفاده از آنها در مراحل تحقیقات جنایی مجاز نیست .

۲– نظر به اوضاع واحوال موجود در قضیه، چنین عمل تحقیقاتی طبق قوانین دولت تقاضا شده موجه نیست البته در معاضدت متقابل نیز شرط مجرمیت متقابل وجود دارد لذا لزوم یکپارچه کردن قوانین کیفری ماهوی احساس می‌شود.

۵-۱-۲ دیگرجنبه‌های جرم رایانه

در فصل پنجم یا فصل نهایی برخی جنبه‌های دیگر جرم رایانه‌ای که بنظر می‌رسد جداگانه باید مورد بحث قرار گیرد به ترتیب زیر بررسی شده است:

الف) ابزارها و تدابیر امنیتی بازدارنده: دراین بخش از دیدگاه جرم شناختی، بمنظور پیشگیری از وقوع جرایم رایانه‌ای به توسعه تدابیر امنیتی و ابزارهای بازدارنده توجه شده است و توصیه شده که دول عضو باید سطح پیشرفته‌ای از تدابیر امنیتی را به کار گیرند و نیز به آموزش و ارائه تسهیلات به افراد مربوط اقدام‌کنند. کادر پلیس و مأمورین باید آموزش لازم را ببینند و باید مقرراتی وضع شود تا حد این تدابیر، لزوم آن و تخطی از آن مشخص شود. از آنجا که سطح نامتجانس تدابیر امنیتی موجب بروز مشکلات عدیده‌ای از بعد داخلی و بین‌المللی می‌شود، از اینرو یکپارچگی تدابیر و راه‌ها کمک بزرگی به پیشرفت امور و جلوگیری از ارتکاب جرم است.

ب) بزهدیده شدن به واسطه رایانه: جرم رایانه‌ای می‌تواند بر بسیاری از مردم اثر گذارد و هزینه‌های زیادی بسته به نوع جرم را موجب شود. تحقیقاتی در چند کشور مشخص می‌سازد بیشتر بزهدیدگان در بخش مسایل مربوط به بانک یا بیمه و در واحدها یا سازمانهای حکومتی یافت می شوند و غالباً بزهدیدگان از گزارش کردن طفره می روند. همکاری بزه دیده عامل اساسی در مبارزه با جرایم کامپیوتری است عدم گزارش بزهدیدگان دلایل چندی دارد مثلاً ترس از دست دادن کار، تعطیل یا ضرر ما لی موسسه ایجاد تزلزل در عقیده مشتریان آن مؤسسه و اینکه ارزیابی ضرر حاصل از گزارش و پیامدهای آن از ضرر وارد خود جرم بیشتر می‌شود و ... راه‌حل‌های پیشنهادی کمیته بعضاً به قرار زیر است:

- ایجاد تعهد قانونی برای مدیران سازمانها در خصوص ارائه گزارش به پلیس در رابطه با جرایم ارتکاب یافته در محدودهٔ شبکه‌های داده‌پردازی الکترونیک و جرم‌انگاری عدم گزارش.
- ایجاد تعهد برای گزارش نه به پلیس بلکه حداقل و در برخی قضایا به یک عضو متخصص مثلاً یک ناظر. این عضو می‌تواند به عنوان رابط و واسط مقامات قضایی و بزهدیده عمل کند.
- تحت پوشش بیمه قرار گرفتن سیستم‌های داده‌پردازی الکترونیک و شرط اقامه خسارت و دریافت آن از شرکت‌های بیمه گزارش جرم به مقامات است.

ج) تجاوزات به حقوق خصوصی و فردی: کنوانسیون حمایت از داده‌ها در ماده ۱۰ خود مقرر می‌دارد «هر دولت عضو تعهد می‌کند ضمانت اجراها و راه‌حلهای خاصی برای تخلفات از اصول اساسی حمایت از داده‌ها وضع کند.» کمیته به منظور حمایت از حقوق خصوصی و فردی علیه جرایمی که به وسیلهٔ تکنولوژی رایانه‌ای جدید ارتکاب می‌یابد اصول اساسی زیر را پیشنهاد می‌کند:

۱- حمایت باید ابتدا در حقوق مدنی و اداری تدوین شود و حقوق کیفری به عنوان آخرین راه‌حل نگریسته شود. در جایئیکه مقررت حقوق مدنی و اداری کافی برای مبارزه نیست.

۲- مقررات کیفری باید به تشریح اعمال ممنوعه به‌طور فشرده و صریح بپردازند و تناسب و توازن منابع در نظر گرفته شود.

۳- اعمالی که جرم شناخته شده‌اند به‌طور واضح به وسیله قوانین کیفری مربوط تشریح شوند. تکنیک ارجاعی منجر به ابهام در مقررات می‌شود. (اصل وضوح)

۴- انواع تخلفات نسبت به حقوق خصوصی و فردی نباید در یک ماده و مقرره کلی ذکر شود.

۵- فقط تجاوزات رایانه‌ای حقوق خصوصی و فردی باید قابل مجازات باشد و اصل قصد ارتکاب است و اعمال ناشی از بی‌مبالاتی به طور استثناء مورد نظر قرار گیرد.

۶- جرایم کوچک رایانه‌ای علیه حقوق خصوصی و فردی تنها با شکایت بزهدیده یا عامل حمایتی خاص یا مقام حمایتی مربوط قابل تعقیب باشد (اصل شکایت)

۲-۲- توصیه‌نامه R(۹۵) ناظر به مشکلات آیین دادرسی مرتبط با فن‌آوری اطلاعات

مشکلات مربوط به آئین دادرسی جرایم رایانه‌ای، در توصیه نامه R(۸۹) صرفاً مورد اشاره قرار گرفته بود و انجام مطالعات و تحقیقات بیشتر و ارائه رهنمود برای کشورهای عضو به توصیه‌نامه دیگری محول شده بود دو سال پس از آن، در سال ۱۹۹۱ یک کمیته منتخب جدید از متخصصان تحت عنوان کمیته متخصصان مشکلات آیین دادرسی مربوط به جرایم رایانه‌ای، بوسیله

شورای اروپا ایجاد شد که کار خود را در اکتبر سال ۱۹۹۲ آغاز و آن را در آوریل ۱۹۹۵ تکمیل نمود و پیش‌نویس توصیه‌نامه و گزارش توجیهی مربوط به آن را پذیرفته و به کمیته اروپایی مشکلات ناشی از جرم ا رائه داد که پس از تصویب این کمیته، نهایتاً در سپتامبر ۱۹۹۵ کمیته وزاری شورای اروپا توصیه نامه (۹۵) R و گزارش توجیهی آن را به تصویب رساند. این توصیه‌نامه صرفاً اصولی را درزمینه آئین دادرسی کیفری مربوط به فن‌آوری اطلاعات در بردارد. که این موارد به علاوه مسائل مربوط به حقوق جزای ماهوی و نیز حقوق جزی بین‌الملل نهایتاً در کنوانسیون اروپایی جرایم سایبر در ۲۳ سپتامبر ۲۰۰۱ بین کشورهای عضو شورای اروپا تصویب شد که متعاقباً مورد بررسی قرار می؛یرد. لذا در این قسمت به بررسی مختصر این توصیه‌نامه که اولین اقدام شورای اروپا در خصوص مشکلات آیین دادرسی این جرایم می‌باشد، می‌پردازیم.

در این توصیه‌نامه کمیته وزرای شورای اروپا با توجه به موارد چندی از جمله پیشرفت بی‌سابقه فناوری اطلاعات و کاربرد آن در کلیه بخشهای جامعه امروزی، آگاهی از اینکه روابط اقتصادی و اجتماعی روزافزونی از طریق یا با استفاده از سیستم‌های اطلاعاتی الکترونیکی به وقوع خواهند پیوست و در نظر گرفتن اینکه ادله اثبات جرایم رایانه‌ای را می‌توان به وسیله این سیستم‌ها ذخیره و منتقل کرد و اینکه قوانین آئین دادرسی کیفری دول عضو اغلب اختیارات مناسبی را در جریان تحقیقات جنایی، برای تفتیش و گردآوری ادله در این سیستم‌ها مقرر نمی کنند. و فقدان اختیارات ویژه مقتضی، می‌تواند مقامات تحقیق و پیگرد را در انجام صحیح وظایفشان درحین مواجهه با پیشرفت آتی فناوری اطلاعات تضعیف کند و با تشخیص این نیاز که ابزارهای قانونی که طبق قوانین دادرسی کیفری به مقامات تحقیق اعطا می‌شوند، باید با طبع ویژه تحقیقات در سیستم‌های اطلاعات الکترونیکی سازگار شوند، همچنین با درک ضرورت تقویت همکاری بین‌المللی و نیل به سازش وسیع‌تر قوانین آیین دادرسی کیفری کشورها در این زمینه، به دولتهای کشورهای عضو توصیه می‌کند که در زمان تجدید نظر قانون و رویه داخلی خود از اصول ضمیمه شده به این توصیه نامه رهنمود بگیرند.

۱-۲-۲- اصول توصیه‌نامه در خصوص آیین دادرسی کیفری مربوط به فناوری اطلاعات

توصیه‌نامه حاوی ۷ فصل و ۱۸ اصل می‌باشد. که عین اصول در این قسمت بیان می‌گردد.

فصل ۱- تفتیش و توقیف

اصل ۱- تمایز حقوقی بین تفتیش سیستم‌های رایانه‌ای و توقیف داده‌های ذخیره شده در آن‌ها و شنود الکترونیکی داده در جریان انتقال، باید به روشنی مطرح و به کار گرفته شوند.

اصل ۲- قوانین آیین دادرسی کیفری باید به مقامات تحقیق اجازه دهند که تحت شرایط مشابه مانند آن‌چه که طبق اختیارات سنتی تفتیش و توقیف مطرح شده است، سیستم‌های رایانه‌ای را تفتیش و داده‌ها را توقیف کنند. شخص متصدی سیستم باید مطلع شود که سیستم تفتیش شده است و از نوع داده‌هایی که توقیف شده نیز باید آگاهی پیدا کند. راه‌حل های حقوقی که به‌طور کلی برای تفتیش و توقیف مقرر شده‌اند، باید به‌طور یکسان در مورد تفتیش در سیستم‌های رایانه‌ای و در مورد توقیف داده‌های موجود در آن‌ها اجرا شوند.

اصل ۳- در طی اجرای یک تفیش، مقامات تحقیق باید اختیار داشته باشند پیرو تضمین‌های مقتضی، تفتیش را به سایر سیستم‌های رایانه‌ای موجود در محدوده صلاحیت قضاییشان که به‌وسیله یک شبکه به هم متصلند، تعمیم دهندو داده‌های موجود در آن‌ها را توقیف کنند، مشروط بر آن‌که اقدام فوری لازم باشد.

اصل ۴– در صورتی که داده‌ها به طور خودکار پردازش شود و از لحاظ عملکرد با یک سند سنتی برابر باشد، مقررات موجود در آیین دادرسی کیفری مربوط به تفتیش و توقیف اسناد باید به‌طور یکسان برای آن‌ها اجرا شود.

فصل ۲ – مراقبت فنی

اصل ۵– نظر به همگرایی فناوری اطلاعات و مخابرات، قوانین مربوط به مراقبت فنی به‌منظور تحقیقات جنایی، از قبیل شنود الکترونیکی مخابرات، باید بررسی و اصلاح شوند، تا در صورت لزوم، قابلیت اجرایی خود را تضمین کنند.

اصل ۶– قانون باید به مقامات تحقیق اجازه دهد که در انجام تحقیق درباره جرایم، به تمامی اقدامات فنی لازم برای گردآوری داده‌های در حال انتقال، دسترسی داشته باشند.

اصل ۷– زمانی که داده‌ها در طی انجام تحقیقات جنایی گردآوری شدند و به خصوص زمانی که از طریق شنود الکترونیکی مخابرات به دست آمدند، داده‌هایی که هدف حمایت قانونی است و به‌وسیله یک سیستم رایانه‌ای پردازش شده است، باید به روشی مناسب حفظ شود.

اصل ۸– قوانین آیین دادرسی کیفری باید به‌منظور امکان‌پذیر ساختن شنود الکترونیکی مخابرات، گردآوری داده‌های در حال انتقال در جریان تحقیق پیرامون جرایم خطرناک علیه حریم خصوصی، درستی و قابلیت دسترسی سیستم‌های مخابراتی یا رایانه‌ای، بررسی شوند.

فصل ۴– تعهد برای همکاری با مقامات تحقیق

اصل ۹– پیرو امتیازات قانونی یا حمایت قانونی، اکثر سیستم‌های حقوقی به مقامات تحقیق اجازه می‌دهند که به اشخاص دستور دهند اشیای تحت کنترلشان را که می‌توان آنها را به عنوان ادله به کار برد، تحویل دهند. به سبکی مشابه، مقرراتی باید طرح شود که این اختیار را اعطا کنند و به اشخاص دستور داده شود تا هر داده ویژه‌ای را که در یک سیستم رایانه‌ای، تحت کنترلشان است، به شکلی که مقام تحقیق مقرر کرده است، تسلیم کنند.

اصل ۱۰– پیرو امتیازات قانونی یا حمایت قانونی، مقامات تحقیق باید این اختیار را داشته باشند تا به اشخاصی که داده‌های موجود در یک سیستم رایانه‌ای تحت کنترلشان است، دستور دهند که کلیه اطلاعات لازم برای دستیابی پیدا کردن به یک سیستم رایانه‌ای و داده‌های موجود در آن‌ها را ارائه کنند. آیین دادرسی کیفری باید تضمین کند که می‌توان به اشخاص دیگری که درباره عملکرد سیستم رایانه‌ای یا اقدامات به کار رفته برای حفظ داده‌های موجود در آن آگاهی دارند، دستور مشابهی بدهد.

اصل ۱۱– الزامات ویژه‌ای باید بر متصدی‌های شبکه‌های خصوصی و همگانی اعمال شوند که خدمات مخابراتی را به عموم ارائه می‌کنند تا به کلیه اقدامات فنی ضروری دسترسی پیدا کنند که مقامات تحقیق را قادر به شنود الکترونیکی مخابرات می‌کند.

اصل ۱۲– الزامات ویژه‌ای باید بر ارائه کنندگان خدماتی اعمال شود که خدمات مخابراتی را از طریق شبکه‌های خصوصی یا همگانی به عموم ارائه می‌کنند تا اطلاعاتی را ارائه می‌کنند تا اطلاعات را ارائه کنند که، وقتی از سوی مقام تحقیق صالح قرار صادر شود، به شناسایی کاربر کمک می‌کنند.

فصل ۴- ادله الکترونیکی

اصل ۱۳- نیاز مشترک به گردآوری، حفظ و ارائه ادله الکترونیکی به روش‌هایی که به بهترین وجه، درستی و صحت انکار ناپذیر آن‌ها را تضمین می‌کند، هم برای هدف‌های تعقیب داخلی و هم برای همکاری بین‌المللی، باید به رسمیت شناخته شود. بنابراین، رویه‌ها و روش‌های فنی برای کنترل ادله الکترونیکی باید بیشتر توسعه داده شود، به خصوص به روشی که سازگاری آن‌ها بین دولتها، تضمین شود. مقررات آیین دادرسی کیفری در زمینه ادله اثبات سنتی باید به‌طور مشابهی برای داده‌های ذخیره شده در یک سیستم رایانه‌ای اجرا شود.

فصل ۵- استفاده از رمزنگاری

اصل ۱۴- تدابیری باید اتخاذ شود تا تأثیر منفی کاربرد رمزنگاری رادر زمینه تحقیق پیرامون جرایم کیفری کاهش دهد، بدون آن که بر استفاده قانونی آن بیشتر از آن‌چه که ضرورت دارد تأثیر بگذارد.

فصل ۶- تحقیق، آمار و آموزش

فصل ۱۵- احتمال خطر ملازم توسعه و کاربرد فناوری اطلاعات در خصوص ارتکاب جرایم کیفری باید پیوسته ارزیابی شود و به‌منظور آگاه ساختن مقامات صالح از پدیده‌های جدید در زمینه جرایم مربوط به رایانه و برای توسعه دادن تدابیر متقابل مقتضی، گردآوری و تجزیه و تحلیل داده‌ها در این جرایم، از جمله طرز برخورد و جنبه‌های فنی، باید بیشتر شود.

اصل ۱۶- راه‌اندازی و ایجاد واحدهای متخصص برای تحقیق کردن پیرامون جرایمی، که مبارزه با آن‌ها مستلزم تخصص ویژه در فناوری اطلاعات است، باید مدنظر قرار گیرد. برنامه‌های آموزشی که پرسنل عدالت کیفری را قادر می‌سازد از تخصص در این زمینه استفاده کنند، باید بیشتر شود.

فصل ۷- همکاری بین‌المللی

اصل ۱۷- اختیار بسط و توسعه یک تفتیش به سیستم‌های رایانه‌ای دیگر، زمانی باید قابل اجرا باشد که سیستم مذکور در یک سیستم قضایی خارجی واقع شده است، مشروط بر آن که اقدام فوری لازم باشد. به‌منظور اجتناب از نقض احتمالی استقلال حاکمیت دولت یا حقوق بین‌الملل، باید یک مبنای حقوقی غیر مبهم برای چنین تفتیش و توقیفی تأسیس شود. بنابراین، لازم است که هر چه زودتر درباره توافق نامه‌های بین‌المللی مذاکره شود تا پی ببریم که چه‌گونه، چه‌وقت و تا چه حد چنین تفتیش و توقیفی باید مجاز شود.

اصل ۱۸- رویه‌های تسریع شده و مناسب و همچنین سیستم مقتضی باید در دسترس باشد که بر طبق آن، مقامات تحقیق بتوانند از مقامات خارجی تقاضا کنند که بدون معطلی ادله را گردآوری کنند. برای چنین منظوری مقامات دریافت‌کننده تقاضا باید مجاز باشند که یک سیستم رایانه‌ای را تفتیش کنند و داده‌ها را به‌منظور انتقال بعدی آن توقیف کنند. مقامات دریافت کننده تقاضا همچنین باید مجاز شوند که داده‌های در حال انتقال مربوط به یک مخابرات ویژه را ارائه کنند، یک مخابرات ویژه را شنود الکترونیکی کنند یا منبع آن را شناسایی کنند. برای چنین منظوری، ابزار و اسناد معاضدت قانونی متقابل باید تکمیل شود.

۲-۲-۲- گزارش توجیهی

در گزارش توجیهی توصیه‌نامه که توسط کمیته اروپایی در زمینه مشکلات جرایم (CDPC) ارائه و به تصویب رسید تحت ۵ عنوان به بررسی مسائل پرداخته شده است.

پس از بیان مختصری از پیشینهٔ تاریخی اقدامات انجام شده، در قسمت مقدمه پس از توجه به پیشرفت فناوری اطلاعات که نتیجه توسعه در قلمرو سیستم‌های رایانه‌ای و مخابرات می‌باشد و ایجاد شبکه‌های رایانه‌ای که محیط کاملاً جدیدی را برای کاربران بوجود آورده‌اند و اینکه در آینده نزدیک در فضای سایبر (Cyber space) ، مرزهای فیزیکی برداشته شده و شاه‌راه‌های اطلاعاتی الگوهای اجتماعی و اقتصادی سنتی را تغییر خواهند داد و به همین میزان مجرمان نیز می‌توانند به عنوان کاربران شبکه‌های رایانه‌ای از امکانات این سیستم بهره ببرند و مرتکب جرم شوند تأکید شده است که به منظور تحقیقات جنایی جرایم مربوط به رایانه و کسب داده‌های معین از شبکه‌ها و سیستم‌های رایانه‌ای نیاز به اختیارات ویژه و همچنین اصلاح قوانین آئین دادرسی کیفری می‌باشد. ضمن اینکه هماهنگی در قوانین نیز ضروری می‌باشد.

همچنین در این قسمت پاره‌ای اصطلاحات مانند رایانه و شبکه‌های رایانه‌ای، داده و اطلاعات، شبکه‌های عمومی و خصوصی تعریف و توضیح داده شده است.

در مورد اصطلاح «**جرایم مربوط به فن‌آوری اطلاعات**» توضیح داده شده که این اصطلاح باید در وسیع ترین معنای ممکن درک شود و شامل جرایمی است که می‌توان به وسیله یک سیستم رایانه‌ای مرتکب شد که سیستم هم می‌تواند هدف یا محیط جرم باشد و به علاوه سیستم‌هایی که عنصری از ارتکاب جرم نیستند ولی محیطی هستند که ادله جرمی را می‌توان در آن یافت نیز جزء این گروه می‌باشند. بنابراین موضوعات آئین دادرسی کیفری جرایم مربوط به فناوری اطلاعات دربرگیرنده هر جرم کیفری است که برای تحقیقات مربوط به آن باید به اطلاعاتی دستیابی پیدا کرد که در سیستم‌های رایانه‌ای پردازش یا منتقل شده‌اند.

در عنوان سوم گزارش محتوای توصیه‌نامه و در عنوان پنجم **تفسیر هر یک از اصول** توصیه‌نامه به تفصیل ذکر شده است (ضمن بیان هدف و محدوده و اصل، تمایزات و جهات اشتراک آنها با مقررات سنتی نیز توضیح داده شده است.)

در عنوان چهارم گزارش بر دو مسئله مشکل‌آفرین که از محدوده اختیارات کمیته خارج بود و لازم بود به تبع توصیه‌نامه به آنها پرداخته شود ذکر گردیده است که شامل: ۱- **مسائل مربوط به همکاری بین‌الملل** (برای مثال مجاز بودن تفتیش شبکه‌های فرامرزی) و ۲- **مسئولیت کیفری دارندگان یا متصدیان** سیستم‌های تابلوی اعلانات (BBS) . در خصوص انتشار اطلاعات یا داده‌هایی که محتوای مجرمانه یا خطرناک دارند[۷]. که این مسائل متعاقباً مورد توجه شورای اروپا قرار گرفته و در کنوانسیون جرایم سایبر و نیز دستورالعمل‌های که به آن اشاره خواهد شد مقرراتی تدوین و به دول عضو پیشنهاد گردیده است.

۷- جهت اطلاعات بیشتر می‌توان به «آیین دادرسی کیفری جرایم رایانه‌ای» خبرنامه انفورماتیک ش: ۸۱- ۸۲ و ۸۳ مراجعه نمود.

۳-۲- کنوانسیون جرایم سایبر[8]

کنوانسیون جرایم سایبر در ۲۳ سپتامبر ۲۰۰۱ در بوداپست به تصویب شورای ارو پا رسید. و از آن به بعد مبنای روابط بین اعضای شورا و سایر کشورهای جهان، این شورا می‌باشد. از آنجا که طبق اعلام شورای مزبور این کنوانسیون طرح کنوانسیون سازمان ملل برای سایر کشورها نیز خواهد بود، اهمیت مضاعف آن را می‌رساند.

شورای اروپا در این کنوانسیون ضمن بیان ضرورت یک سیاست جنایی عمومی به عنوان یک اولویت در حمایت از جامعه در برابر جرائم سایبر، از قبیل تصویب قوانین مناسب و گسترش همکاری بین‌المللی، با توجه به تغییرات عمیقی که بواسطه دنیای دیجیتال و شبکه‌های رایانه‌ای در جهان امروز به وجودآمده و اظهار نگرانی از استفاده از شبکه‌های رایانه‌ای و اطلاعات الکترونیکی بوسیله مجرمان برای ارتکاب جرم یاذخیره یا انتقال دلایل مرتبط با جرم، برای مبارزه مؤثر با جرایم سایبر خواستار همکاری بین‌المللی فزاینده در زمینه‌های کیفری شده است.

شورای اروپا در این کنوانسیون به عنوان یک قانون مؤثر برای مقابله با اینگونه جرایم، مفاهیم اساسی حقوق بشر مذکور درکنوانسیون ۱۹۵۰ شورای اروپا برای حمایت از حقوق بشر و آزادیهای اساسی ، میثاق بین‌المللی سازمان ملل در زمینه حقوق سیاسی و مدنی (۱۹۶۶) و سایر معاهدات بین‌المللی حقوق بشر در زمینه حق آزادی عقیده، شامل آزادی تحقیق، دریافت و بیان اطلاعات و ایده‌ها از هر نوع بدون ملاحظه مرزها و آزادی بیان و حقوق مربوط به احترام به حریم خصوصی اشخاص، را محترم شمرده است. همچنین کنوانسیون ۱۹۸۱ شورای اروپا در مورد حمایت از داده‌های شخصی و کنوانسیون سازمان ملل متحد درباره حقوق کودک (۱۹۸۹) و کنوانسیون سازمان بین‌المللی کار درباره بدترین اشکال کار کودکان (۱۹۹۹) مورد توجه در این کنوانسیون بوده‌اند.

این کنوانسیون دربردارنده ابعاد مختلف جرایم سایبری از حیث حقوق جزای ماهوی – حقوق جزای شکلی و حقوق جزای بین‌المللی می‌باشد.

کنوانسیون حاوی ۴ فصل می‌باشد: فصل ۱ـ کاربرد اصطلاحات؛ که اصطلاحات سیستم رایانه‌ای داده رایانه‌ای ـ ارائه دهنده خدمات و داده ترافیک را تعریف نموده است.

فصل ۲- «تدابیری که در سطح ملی باید رعایت شود» دربردارنده . دو بخش حقوق جزای ماهوی و حقوق جزای شکلی است. فصل ۳- «همکاری بین‌الملل » و فصل ۴- «مقررات نهایی» است که در این فصل مراحل امضاء و لازم‌الاجرا شدن، الحاق به کنوانسیون، آثار کنوانسیون، اصلاحات، حل و فصل منازعات و ... آمده است. که با توجه به اهمیت محتوای فصول دوم و سوم مورد بررسی قرار می گیرد.

۸- Cyber crime

جرایم در فضای سایبر یا جرایم سایبری که به واسطه تغییرات سریع فناوری اطلاعات در قلمرو سیستم‌های رایانه‌ای و نیز مخابرات و تجمیع رایانه، مودم و مخابرات (اعم از ماهواره و ...) با حالات شبیه‌سازی و مجازی سازی امکان وقوع یافته‌اند. در این جرایم تأکید بر رایانه نیست بلکه رایانه خود وسیله ارتکاب جرم است و تحت عنوان نسل سوم جرایم رایانه‌ای ذکر می‌شوند. جهت اطلاعات بیشتر به مقاله «مقدمه‌ای بر ماهیت و تقسیم‌بندی تئوریک جرایم رایانه‌ای» نوشته محمدحسن دزیانی، خبرنامه انفورماتیک ش ۸۷ رجوع شود.

۱-۳-۲- مقررات کنوانسیون در حقوق جزای ماهوی

بخش اول فصل دوم کنوانسیون دربردارنده مقررات حقوق جزای ماهوی است مواد ۲ الی ۱۰ انواع جرایم را است و مواد ۱۱ الی ۱۳ نیز مقررات کلی مربوط به همه جرایم را تحت عنوان ضمانت اجراها و مسئولیتهای تبعی بیان داشته است.

۱-۱-۳-۲- انواع جرایم

جرائم مذکور در کنوانسیون تحت ۴ عنوان به شرح زیر آمده‌اند:

۱- جرایم علیه محرمانگی، تمامیت و در دسترس بودن سیستم‌ها و داده‌های رایانه‌ای

- دسترسی غیر قانونی[۹] (ماده ۲): هر نوع دسترسی عمدی بدون حق به تمام یا قسمتی از سیستم رایانه‌ای (ممکن است عضو مورد نظر مقرر دارد جرم در اثر تعرض به اقدامات امنیتی با قصد دسترسی به داده‌های رایانه‌ای یا دیگر مقاصد ناروا یا نسبت به سیستم رایانه‌ای که با سیستم رایانه‌ای دیگری در ارتباط می‌باشد، محقق شود.)

- شنود غیر قانونی[۱۰] (ماده ۳): هر نوع شنودعمدی و بدون حق و از طریق ابزارهای فنی انتقال داده‌های رایانه‌ای غیر عمومی که به سیستم رایانه‌ای یا از طریق آن ارسال شده یا در آن موجود می‌باشد. (ممکن است عضو مورد نظر مقرر دارد این جرم با دارا بودن قصد ناروا یا نسبت به سیستم رایانه‌ای که با سیستم دیگری در ارتباط است محقق شود)

- **ایجاد اختلال در داده‌ها**[۱۱] (ماده ۴): هر نوع صدمه زدن[۱۲]، پاک کردن[۱۳]، خراب کردن[۱۴] ، تغییر[۱۵] یا متوقف کردن داده‌های[۱۶] رایانه‌ای که به‌طور عمدی و بدون حق انجام شود. (ممکن است عضو مورد نظر این جرم را محدود کند به جایی که صدمه شدیدی وارد شده باشد)

- **ایجاد اختلال در سیستم**[۱۷] (ماده ۵): هر نوع ایجاد اشکال جدی عمدی و بدون حق که در عملکرد سیستم رایانه‌ای در اثر وارد کردن، انتقال، صدمه زدن، پاک کردن، خراب کردن، تغییر یا متوقف کردن داده‌های رایانه‌ای بوجود می‌آید.

- **سوءاستفاده از دستگاه‌ها**[۱۸] (ماده ۶): شامل هر یک از اقدامات عمدی و بدون حق زیر:

الف) تولید، فروش، تهیه برای استفاده، وارد کردن، توزیع یا به نحو دیگری در دسترس قرار دادن موارد زیر:

۱) دستگاهی که برنامه رایانه‌ای دارد، اساساً به منظور ارتکاب هر یک از جرایم مندرج در مواد ۲ تا ۵ (جرایم فوق‌الذکر) طراحی یا انطباق داده شده است.

۹- Illegal access
۱۰- Illegal Interception
۱۱- Data interference
۱۲- Damaging
۱۳- Deletion
۱۴- Deterioration
۱۵- Alteration
۱۶- suppression
۱۷- system interference
۱۸- Misuse of devices

۲) گذر واژه رایانه‌ای، کد دسترسی، یا داده مشابهی که بوسیله آن تمام یا قسمتی از سیستم رایانه‌ای قابل دسترسی است و به قصد ارتکاب هر یک از جرایم مندرج در مواد ۲ تا ۵ (جرایم فوق‌الذکر) مورد استفاده قرار گیرد.

ب) در اختیار داشتن هر یک از مواد مندرج در بند الف (۱) یا الف (۲) با قصد سوء استفاده از آنها جهت ارتکاب هر یک از جرایم مقرر در مواد ۲ تا ۵ (جرایم فوق‌الذکر) (ممکن است شرط در تصرف داشتن برای مسئولیت کیفری بار شود)

ضمناً تأکید شده در جاییکه تولید، فروش، تهیه برای استفاده وارد کردن یا توزیع یا دیگر مواد در اختیار یا در تصرف داشتن موارد مندرج در بند یک برابر ارتکاب جرایم مقرر فوق مورد استفاده قرار نمی‌گیرد، نباید مسئولیت کیفری اعمال شود.

۲- جرایم مرتبط با رایانه

– **جعل مرتبط با رایانه**[۱] (ماده ۷) : هر نوع وارد کردن، تغییر، حذف یا موقوف‌سازی عمدی و بدون حق داده‌های رایانه ای که منجر به ایجاد داده‌های غیر معتبر می‌شود با همان قصدی که از آن انتظار می‌رود یا در راستای اهداف غیر قانونی به عنوان داده‌هایی که از اعتبار کافی برخوردارند بکار گرفته شوند، چه آن داده‌ها به‌طور مستقیم قابل درک و خواندن باشند یا نباشند. (عضو مورد نظر می‌تواند مقرر دارد که وجود قصد فریب یا دیگر مقاصد ناروا پیش از اتصاف مسئولیت کیفری ضروری است.)

– **کلاهبرداری مرتبط با رایانه**[۲] (ماده ۸): هرگونه اقدامات عمدی بدون حق زیر که به قصد فریب یا دیگر مقاصد ناروا و در راستای جلب منفعت اقتصادی بدون حق برای خود یا دیگری صورت می‌پذیرد:

الف) هر گونه وارد کردن، تغییر، حذف یا موقوف‌سازی داده‌های رایانه‌ای

ب) هرگونه ایجاد اختلال در عملکرد یک سیستم رایانه‌ای

۳- جرایم مرتبط با محتوا[۳]

« جرائم مرتبط با هرزه‌نگاری کودکان» (ماده ۹) هرگونه اقدامات عمدی و بدون حق ذیل:

الف) تولید هرزه‌نگاری کودکان به قصد توزیع از طریق سیستم رایانه‌ای

ب) ارائه یا در دسترس قرار دادن هرزه‌نگاری کودکان از طریق سیستم رایانه‌ای

ج) توزیع یا انتقال هرزه‌نگاری کودکان از طریق سیستم رایانه‌ای

د) تهیه هرزه‌نگاری کودکان از طریق سیستم رایانه‌ای برای خود یا دیگری

ه) در اختیار داشتن هرزه‌نگاری کودکان بر روی سیستم رایانه‌ای یا رسانه ذخیره‌ساز داده رایانه‌ای واژه «هرزه‌نگاری کودکان» شامل موضوعات مستهجنی می‌شود که به صورت تصویری و به طرق ذیل نمایش داده می‌شود:

الف) صغیری که به‌طور آشکار در حال ارتکاب عمل جنسی است.

ب) شخصی که به عنوان یک صغیر ظاهر می‌شود و به‌طور آشکار در حال ارتکاب عمل جنسی است.

ج) تصاویر واقعی که نشان می‌دهد یک صغیر به‌طور آشکار در حال ارتکاب عمل جنسی است.

واژه «صغیر» شامل تمام افراد زیر ۱۸ سال است. در ماده مقرر شده است که می‌توان محدودیت سنی کمتری که البته نباید از ۱۶ سال کمتر باشد، توسط کشور عضو تعیین شود و همچنین هر عضو می‌تواند حق عدم اجرای تمام یا قسمتی از بندهای دو قسمت اول و ب و ج قسمت اخیر را برای خود محفوظ دارد.

۴- جرایم مرتبط با تعرض به حق نشر و حقوق مربوط به آن

جرایم مرتبط با تعرض به حق نشر و حقوق مربوط به آن (ماده ۱۰):

۱) هرگونه تعرض به حق نشر که به‌طور عمدی و به‌خاطر انگیزه‌های تجاری و بوسیله سیستم‌های رایانه ای صورت می‌گیرد.

اینگونه موارد نقض باید مطابق مقرراتی تدوین شود که در معاهده پاریس (۲۴ جوی ۱۹۷۱) کنوانسیون برن درباره حمایت از آثار ادبی و هنری و معاهده حق نشر سازمان جهانی ما لکیت معنوی (WIPO) و جنبه‌های تجارتی مرتبط با حقوق مالکیت معنوی مورد قبول دولتهای عضو واقع شده است.

۲) هرگونه تعرض به حقوق مرتبط با حق نشر که به‌طور عمدی و به خاطر انگیزه‌های تجاری و بوسیله سیستم‌های رایانه‌ای صورت می‌گیرد.

جرم‌انگاری این موارد باید مطابق با مقررات کنوانسیون بین‌المللی حمایت از اجراکنندگان، تولیدکنندگان آثار صوتی و سازمان‌های صدا و سیما که در شهر رم برگزار شد (کنوانسیون رم) و موافقتنامهٔ ابعاد تجاری مرتبط با مالکیت معنوی و معاهده مربو

ط به آثار صوتی و اجرائات سازمان جهانی مالکیت معنوی باشد.

البته در قسمت سوم این ماده مقرر شده که دولتهای عضو تحت شرایط محدودی می‌توانند مسئولیت کیفری برای موارد فوق قائل نشوند مشروط به اینکه ضمانت اجراهای مؤثر دیگری در این زمینه پیش‌بینی کرده باشند.

۲-۱-۳-۲- ضمانت اجراها و مسئولیت‌های تبعی

عنوان پنجم از بخش اول کنوانسیون مواد ۱۱ الی ۱۳ حاوی مقرات کلی مربوط به همه جرائم است که شامل موضوعات زیر می‌شود:

۱- شرکت و معاونت در جرم:

بند ۱ – ماده ۱۱ : کنوانسیون مقرر نموده است که هرگونه معاونت یا مشارکت عمدی در ارتکاب هر یک از جرایم مندرج در این کنوانسیون جرم بوده و باید در حقوق داخلی جرم‌انگاری شود.

۲- شروع به جرم:

در بند ۲ ماده ۱۱ شروع به جرم عمدی جرایم مندرج در مواد ۳ تا ۵، ۷، ۸، ۹ (۱) – الف و ۹ (۱) ج کنوانسیون را جرم‌انگاری نموده و البته در این خصوص برای کشورهای عضو این حق را قائل شده که تمام یا قسمتی از این بند (شروع به جرم) را اجرا ننمایند.

۳- مسئولیت شخصی حقوقی

بموجب ماده ۱۲ کنوانسیون، ۱) شخص حقوقی را به خاطر ارتکاب جرایم مصوب مندرج در این کنوانسیون که در راستای منافع خود مرتکب شده باید تحت تعقیب کیفری قرار داد. در صورتیکه این عمل توسط شخص حقیقی که شخصاً یا به عنوان بخشی از ارگان شخص حقوقی به فعالیت می‌پردازد ارتکاب یافته و پست مدیریت و رهبری آن شخصیت حقوقی را به عهده دارد و اختیارات ذیل را داراست:

الف) اختیار نمایندگی شخص حقوقی

ب) اختیار تصمیم‌گیری شخص حقوقی

ج) اختیار اعمال نظارت بر شخص حقوقی

۲- در جایی که خلاء سرپرستی یا نظارت شخص حقیقی مندرج در پاراگراف فوق وجود دارد و این امکان فراهم آمده که جرایم مصوب کنوانسیون توسط شخص حقیقی دیگری براساس اختیارات خود در آن مجموعه ارتکاب یابد. امکان اعمال مسؤولیت بر آن مجموعه وجود داشته باشد.

۳- مسئولیت شخص حقوقی با توجه به اصول قانونی حاکم بر هر دولت عضو ممکن است کیفری مدنی یا اداری تعیین شود.

۴- اعمال مسئولیت بر شخص حقوقی نباید موجب تحت الشعاع قرار گرفتن مسئولیت اشخاص حقیقی شود که مرتکب جرایم مربوط شده‌اند.

۴- ضمانت اجراها و تدابیر قانونی

ماده ۱۳ کنوانسیون مقرراتی در مودر نحوه تعیین مجازات تصویب شده است:

۱- جرایم مندرج مصوب در این کنوانسیون باید با مجازاتهای مؤثر، بازدارنده و مناسب که شامل مجازات سا لب آزادی می‌شود، قابلیت کیفر داشته باشند.

۲- اشخاص حقوقی باید مطابق ماده ۱۲ قابلیت اتصاف مسئولیت کیفری را پیدا کنند و با بکارگیری ضمانت اجراهای کیفری و غیر کیفری مؤثر، بازدارنده و مناسب از قبیل جزای نقدی مجازات شوند.

۲-۳-۲- مقررات کنوانسیون در آیین دادرسی کیفری

بخش دوم فصل دوم کنوانسیون به این مقررات اختصاص دارد و تحت ۵ عنوان از ماده ۱۴ تا ۲۱ را دربرمی‌گیرد.

۱-۲-۳-۲- مقررات عمومی

در ماده ۱۴ کنوانسیون، دولتهای عضو متعهد شده‌اند که مقررات لازم برابر اجرای اختیارات و رسیدگی‌های قضایی مندرج در این بخش را به منظور پی‌جویی و رسیدگی های کیفری ویژه وضع نمایند.

همچنین قلمرو اعمال مقررات فوق را در سه مورد ذیل دانسته است:

الف) جرایمی که مطابق مقررات این کنوانسیون به تصویب رسیده است،

ب) سایر جرایمی که از طریق یک سیستم رایانه‌ای ارتکاب می‌یابد، و

ج) جمع‌آوری ادله الکترونیک راجع‌به فعل مجرمانه.

و در ماده ۱۵ مقرر شده است که تصویب، اجرا و بکارگیری اختیارات و رسیدگی‌های قضایی پیش‌بینی شده در این بخش در حقوق داخلی باید به گونه‌ای باشد که در راستای حمایت از حقوق و آزادی‌های بشری است که برخاسته از تعهدات اعضاء به موجب کنوانسیون شورای اروپا (۱۹۵۰) در زمینه حمایت از حقوق و آزادی‌های اساسی بشر و میثاق حقوق مدنی و سیاسی سازمان ملل متحد ۱۹۴۶ و دیگر اسناد بین‌المللی حمایت از حقوق بشر که قابلیت اجرا دارند، می‌باشد. همچنین باید تاحدی که سازگار با منافع عمدی است، تأثیر اختیارات و رویه‌های مقرر بر حقوق، مسئولیتها و منافع مشروع اشخاص ثالث نیز در نظر گرفته شود.

۲-۲-۳-۲- حفاظت سریع از داده‌های رایانه‌ای ذخیره شده

بموجب ماده ۱۶ کنوانسیون، جهت محافظت و نگهداری داده‌های رایانه‌ای خاص نظیر داده ترافیک[۱۹] که در یک سیستم رایانه‌ای ذخیره شده است و در معرض صدمه یا تغییر قرار دارند، مقامات ذیصلاح می‌توانند دستوراتی را صادر نمایند. و شخص را ملزم کند تا دوره زمانی مشخص (حداکثر ۹۰ روز که قابل تمدید نیز می‌باشد) اقدام به محافظت و نگهداری از داده‌های رایانه‌ای و حفظ تمامیت آنها و همچنین محرمانه نگهداشتن آنها بنماید.

در ماده ۱۷ نیز تحت عنوان حفاظت سریع و افشای محدود داده ترافیک، ارائه دهندگان خدمات[۲۰] ملزم به حفاظت سریع از داده ترافیک شده و همچنین ملزم می‌باشند که داده ترافیک را به نحویکه امکان شناسایی ارائه دهندگان خدمات و مسیری که از طریق آن ارتباط برقرار شده است را برای مقامات ذ یصلاح افشاء نمایند.

۳-۲-۳-۲- دستور تولید

بموجب ماده ۱۸ کنوانسیون مقامات ذیصلاح اختیار صدور دستور در موارد ذیل را دارند:

الف) به شخصی که در قلمرو یک عضو، داده‌های رایانه‌ای ویژه‌ای را تحت کنترل و اختیارش است و در سیستم رایانه‌ای یا رسانه ذخیره ساز داده‌های رایانه‌ای ذخیره شده دستور تسلیم آنها را بدهند.

ب) به ارائه دهنده خدماتی که خدماتش را در قلمرو عضو مورد نظر ارائه می‌دهد، دستور تسلیم اطلاعات متعلق به مشترکی که مرتبط با آن خدمات است و در محدودهٔ تحت کنترل آن ارائه دهنده خدمات است را صادر نمایند.

منظور از «اطلاعات متعلق به مشترک» هرگونه اطلاعات که در قالب داده‌های رایانه‌ای یا دیگر اشکال می‌باشد که توسط ارائه دهنده خدمات درباره مشترکین خود نسبت به خدماتش نگهداری می‌شود و شامل داده ترافیک یا داده محتوا نمی‌شود و دربردارنده: الف) نوع خدمات ارتباطی، پیش‌نیازهای فنی که در مورد آن به کار رفته و دوره استفاده از آن خدمات؛ ب) مدیریت مشترک، آدرس جغرافیایی یا پستی، شماره تلفن و سایر شماره‌های دسترس اطلاعات مربوط به قبوض و پرداخت که بر پایه قرار داد یا ترتیب خدمات موجود است.

ج) دیگر اطلاعات راجع به محل نصب تجهیزات ارتباطات که براساس قرارداد یا ترتیب خدمات در دسترس قرار می‌گیرد.

۴-۲-۳-۲- تفتیش و توقیف داده‌های ذخیره شده

در ماده۱ ۹ مقررات مربوط به تفتیش و توقیف داده‌های رایانه‌ای ذکر شده است از جمله مقرر شده است: اولاً در صورت تفتیش سیستم رایانه‌ای یا بخشی از آن توسط مقامات ذیصلاح اگر دلایلی در اختیار دارند مبنی بر این اعتقاد که داده مورد نظر آنها در سیستم رایانه‌ای دیگری در منطقه تحت قلمرو آن کشور قرار دارد و از سیستم اولیه بطور قانونی قابل دسترسی هستند، این مقامات صلاحیت گسترش تفتیش یا دیگر اقدامات مشابه به سیستم ثانویه را نیز باید دارا باشند.

۱۹- داده ترافیک: بوجب ماده یک کنوانسیون عبارتست از: هرگونه داده رایانه‌ای که مرتبط با ارتباط برقرار شده از طریق سیستم رایانه‌ای می‌باشد. این داده را سیستم رایانه‌ای بوجود می‌آورد که بخشی از زنجیره ارتباطی را تشکیل می‌دهد. این داده بعدها، مقصد مسیر، مدت، تاریخ، اندازه، دوام یا نوع خدمات اصلی ارائه شده را نشان می‌دهد.

۲۰- منظور از «ارائه دهنده خدمات» در کنوانسیون هر مجموعه خصوصی یا عمومی است که برای کاربر خدمات خود امکان برقراری ارتباط از طریق سیستم رایانه‌ای را فراهم می‌آورد و نیز هر مجموعه دیگری است که داده رایانه‌ای را به جای ارائه دهنده خدمات ارتباطی یا کاربران اینگونه خدمات، پردازش یا ذخیره می‌کند.

ثانیاً در صورت نیاز به توقیف یا دیگر دسترسی‌های امنیتی مشابه نسبت به داده‌های رایانه‌ای مقامات ذیصلاح اختیارات ذیل را باید دارا باشند:

- توقیف یادیگر اقدامات امنیتی مشابه نسبت به سیستم رایانه‌ای یا قسمتی از آن
- ایجاد و حفظ یک نسخه کپی از داده‌های رایانه‌ای مورد نظر
- حفاظت از تمامیت داده‌های رایانه‌ای ذخیره شده مربوطه و
- غیر قابل دسترس کردن یا حذف آن داده‌ها از روی سیستم رایانه‌ای در دسترس

ثالثاً – مقامات ذیصلاح اختیار دارند در صورت لزوم به شخصی که اطلاعاتی درباره عملکرد سیستم رایانه‌ای یا ویژگی حفاظتی و امنیتی اعمال شده بر روی داده‌های رایانه‌ای دارد در صورتی که متعارف و منطقی باشد دستور دهند تا اطلاعات لازم و ضروری را ارائه دهند تا بتوانند اقدام به تفتیش یا توقیف به شرح فوق بشوند.

۵-۲-۳-۲- جمع‌آوری داده‌های رایانه‌ای در زمان واقعی

در ماده ۲۰ کنوانسیون ضمن اینکه به مقامات ذیصلاح این اختیار داده شده است که اقدام به جمع‌آوری یا ضبط داده ترافیک در زمان واقعی که به ارتباط معین اختصاص دارد از طریق بکارگیری ابزارهای فنی بنمایند بلکه می‌توانند ارائه کننده خدمات را ملزم نماینده که در حیطه توانایی فنی خود نسبت به جمع‌اوری یا ضبط از طریق ابزارهای فنی که در اختیار دارد اقدام نماید و یا در این امر با مقامات ذیصلاح همکاری نماید با دستور حفظ محرمانگی و عدم افشاء آنها.

در ماده ۲۱ کنوانسیون مقررات مربوط به **شنود داده محتوا** ذکر شده است، و بموجب آن تنها در مورد جرایم شدیدی که در قوانین داخلی هر کشور معین شده است به مقامات ذیصلاح این اختیار داده شده است که اقدام به جمع‌آوری یا ضبط داده محتوا در زمان واقعی یک ارتباط معین از طریق سیستم رایانه ای که در حوزه قلمرو آن عضو انتقال می‌یابد، بنامید یا ارائه دهنده خدمات را درحیطه توانایی فنی خود ملزم به جمع‌آوری یا ضبط داده‌های فوق یا همکاری و کمک به مقامات ذیصلاح در این مورد بنماید و ضمناً دستور محرمانه تلقی کردن و عدم افشاء آن را نیز صادر نماید.

۳-۳-۲- مقررات مربوط به حقوق جزای بین‌الملل

۱-۳-۳-۲- صلاحیت

بخش سوم فصل دوم کنوانسیون به صلاحیت اختصاص یافته است. در ماده ۲۲ موادیکه رسیدگی به جرم در صلاحیت هر عضو قرار دارد را به شرح زیر مقرر داشته است:

الف) جرم در قلمروش بوقوع پیوسته باشد یا

ب) جرم در کشتی‌هایی به وقوع پیوسته که پرچم آن کشور برافراشته می‌باشد یا

ج) جرم در هواپیماهایی به وقوع پیوسته باشد که مطابق مقررات آن عضو به ثبت رسیده یا

د) در جایی که جرم مورد نظر مطابق قوانین جزایی قابل مجازات شناخته شده توسط تبعه‌اش ارتکاب یافته یا جرم ارتکابی از جمله جرایم واقع در حوزه صلاحیت جهانی حقوق جزا باشد.

همچنین متذکر شده است که این کنوانسیون مانع اجرای هرگونه صلاحیت کیفری که مطابق قوانین داخلی به مرحله اجرا در می‌آید نمی‌شود.

و در موارد تعارض صلاحیت پیشنهاد شده است که در صورت صلاحدید اعضا یکه ادعای صلاحیت دارند به شور نشسته تا مناسب‌ترین و شایسته‌ترین عضو صالح به تعقیب و رسیدگی را تعیین نمایند.

۲-۳-۳-۲- همکاری بین‌المللی

فصل سوم کنوانسیون مواد ۲۳ الی ۳۵ به همکاری بین‌المللی اخصاص یافته است. در ماده ۲۳ مقرر شده است که اعضای کنوانسیون براساس مقررات این فصل و از طریق تمهیدات بین‌المللی مربوط به همکاری بین‌المللی در زمینه موضوعات کیفری و تمهیدات مورد توافق مبتنی بر قانونگذاری یکنواخت یا متقابل و حقوق داخلی باید برای رسیدن به وسیع‌ترین حوزه ممکن پی جویی‌ها یا رسیدگی‌هایی قضایی راجع‌به جرایم مرتبط با سیستم‌های رایانه‌ای و داده‌ها یا جهت جمع‌آوری ادله الکترونیک در جرایم همکاری کنند.

و در ادامه مقررات مربوط به موضوعات ذیل بیان شده است:

- **استرداد مجرمین:** در ماده ۲۴ استرداد در مورد جرایم مندرج در کنوانسیون مشروط به این است که عمل در هر دو دولت جرم‌انگاری شده و مجازات تعیین شده حداقل یکسال حبس باشد، مگر اینکه طبق معاهده بین ۲ یا چند عضو حداقل مجازات کمتر توافق شده باشد. در مواردیکه معاهده استرداد وجود ندارد دول عضو متعهد شده‌اند که این کنوانسیون را مبنای قانونی استرداد در رابطه با جرایم فوق‌الذکر در نظر بگیرند. همچنین در ادامه ماده مقررات مربوط به نحوه اعطای درخواست استرداد و نحوه رسیدگی به آن و ... ذکر شده است.
- **اصول کلی راجع‌به همکاری دو جانبه:** در ماده ۲۵ دول عضو به منظور همکاری دو جانبه در وسیع‌ترین حالت ممکن اقدام به وضع قوانین و مقررات نمایند. همچنین در این ماده در شرایط اضطراری استفاده از ابزارهای سریع ارتباطی نظیر فاکس یا پست الکترونیکی را در نظر گرفته است. و تأکید شده شرایط همکاری دو جانبه باید مطابق با حقوق عضو طرف درخواست یا معاهده همکاری دو جانبه در حال اجرا باشد که لازم است در آنها شرایطی که طرف درخواست می‌تواند از همکاری خودداری نماید نیز ذکر شود.

در ماده ۲۵ ارائه اطلاعات بطور داوطلبانه از سوی هر یک از اعضاء و بدون اینکه درخواستی دریافت شده باشد را مقرر نموده است و عضو ارائه کننده می‌تواند درخواست کند آن اطلاعات بطور محرمانه نگهداری شده یا مطابق شرایطی استفاده شوند. اگر دریافت کننده این شرایط را پذیرفت ملزم به رعایت آنها می‌باشد.

- **آیین دادرسی مرتبط با درخواستهای همکاری دو جانبه در جایی که قراردادهای بین‌المللی قابل اجرا وجود ندارد.** ماده ۲۷ جزئیات مربوط به درخواست‌های همکاری دو جانبه و آیین دادرسی حاکم بر آن را تشریح نموده است و در ماده ۲۸ برای عضو طرف درخواست، حق تعیین شرایطی از جمله محرمانگی و محدودیت در استفاده پیش‌بینی شده است.
- **همکاری دو جانبه در خصوص اقدامات موقت:** موجب ماده ۲۹ کنوانسیون هر یکی از اعضا می‌تواند از عضو دیگر بخواهد دستور یا هر نوع اقدام به حفاظت فوری از داده های ذخیره شده در سیستم رایانه‌ای موجود در قلمرو آن عضو را صادر نماید. همچنین به موجب ماده ۳۰ در جاییکه درخواست حفاظت از داده ترافیک بموجب ماده ۲۹ به اجرا در آمده است باید به حد کافی از داده ترافیک مربوطه در اختیار در خواست کننده قرار بگیرد تا بتواند نسبت به شناسایی ارائه کننده خدمات مذکور و مسیری که از طریق آن ارتباط برقرار شده به کار گیرد.

امتناع از پذیرش مواد مذکور در فوق در دو صورت پذیرفته شده است:

۱- درخواست مربوط به جرمی بوده که طرف درخواست آن را جرمی سیاسی یا مرتبط با جرم سیاسی قلمداد می‌کند.

۲- طرف درخواست اجرای آن را محتمل به ورود لطمه به حاکمیت، امنیت، نظم عمومی یا سایر منافع اساسی‌اش می‌داند.

– **همکاری دو جانبه در راستای اختیارات پی‌جویی:** همکاری دو جانبه در راستای دسترسی به داده‌های رایانه‌ای ذخیره شده در ماده ۳۱ پیش‌بینی شده است که متعاقب درخواست تفتیش یا دسترسی مشابه، توقیف یا اقدامات امنیتی مشابه یا افشای داده‌های ذخیره شده بر روی سیستم رایانه‌ای که در قلمرو عضو دیگر قرار دارد بعمل می‌آید.

دسترسی فرامرزی به داده رایانه‌ای ذخیره شده در اثر رضایت یا از طریق منابع عمومی در دسترس، در ماده ۳۳ مواردی پیش‌بینی شده که بدون اخذ مجوز از اعضای دیگر هر عضو می‌تواند اولاً – بدون در نظر گرفتن موقعیت جغرافیایی داده‌های رایانه‌ای ذخیره شده، با دسترسی به منابع عمومی در دسترس (منبع باز) آنها را بدست آورد ثانیاً – با کسب رضایت شخصی که صلاحیت قانونی افشای داده‌ها از طریق سیستم رایانه‌ای را دارد از طریق سیستم مستقر در قلمرو خود به داده‌های رایانه‌ای ذخیره شده در قلمرو عضو دسترسی پیدا کند یا آنها را دریافت کند.

– **همکاری دو جانبه در زمینه جمع‌آوری داده ترافیک در زمان واقعی:** ماده ۳۳ این نوع همکاری را حداقل در موارد مجرمیت متقابل مقرر داشته است.

– **همکاری دو جانبه در زمینه شنود داده محتوا:** ماده ۳۳ در حدود معاهدات قابل اجرا و حقوق داخلی کشورهای عضو این نوع همکاری را مقرر داشته است.

شبکه

ماده ۳۵ مقرر نموده است که هر یک از اعضاء باید یک مرکز تماس ۲۴ ساعته که در هفت روز هفته در دسترس باشد تأسیس کند تا به‌منظور پی‌جویی‌ها یا رسیدگی‌های کیفری مرتبط با داده‌ها و سیستم‌های رایانه‌ای همکاری فوری ارائه دهد یا در راستای جمع‌آوری ادله الکترونیک مرتبط به خدمت گرفته شود.

۴-۲- دستورالعمل‌های شورای اروپا در مورد مسئولیت کیفری ارائه کنندگان خدمات اینترنتی و جامعه اطلاعاتی

با ظهور و توسعه فزاینده شبکه‌های رایانه‌ای و ارتباطی و انواع خدمات جامعه اطلاعاتی به کاربران موضوع وجود مقررات تنظیمی نسبت به وظایف و مسئولیت‌های این ارائه‌کنندگان خدمات مطرح گردید. به نحویکه درخصوص مسئولیت کیفری آنان این موضوع مورد توجه کمیته متخصصان تدوین کنوانسیون R(۹۵) ناظر به مسائل آیین دادرسی کیفری بعنوان اقدامی که در آینده باید مورد توجه قرار گیرد مطرح شد.

دستورالعمل‌هایی در این خصوص در سالهای اخیر به تصویب شورای اروپا رسیده است که به اختصار مورد اشاره قرار می‌گیرد.

۱-۴-۲- دستورالعمل اروپایی در مورد حریم خصوصی و ارتباطات الکترونیک – ۱۲ جولای ۲۰۰۲[21]

در این دستورالعمل پس از ارائه تعاریف اصطلاحات به موضوعاتی پرداخته شده که اهم آن به قرار زیر است امنیت شبکه: در ماده ۴ دولتهای عضو متعهد شده‌اند که مقرراتی را وضع نمایند که به موجب آن ارائه کنندگان خدمات تدابیر فنی و سازمان

21- European directive on privacy and electronic communications of 12 July 2002

لازم را برای حفظ امنیت شبکه اتخاذ نمایند. و همچنین موظف شوند در موارد خاصی کاربران خود را از خطرات موجود در شبکه آگاه کنند.

محرمانگی ارتباطات: در ماده ۵ مقرر شده است که باید تدابیر فنی و سازمانی خاصی توسط ارائه کنندگان خدمات برای حفظ حریم خصوصی و محرمانگی ارتباطات در برابر مواردی مثل شنود و ... اتخاذ گردد. و در ادامه به تعیین محدوده حریم خصوصی در انواع ارتباطات پرداخته شده است.

ارتباطات ناخواسته: در ماده ۱۳ مقرر شده است که باید کاربران حق جلوگیری از این ارتباطات ناخواسته را داشته باشند و لذا ارائه کنندگان خدمات باید تدابیر لازم را اتخاذ نمایند.

و در ماده ۱۵ حق محدود کردن حقوق فردی مندرج در این دستورالعمل در موارد زیر برسمیت شناخته شده است: امنیت ملی ـ دفاع اجتماعی و پیشگیری، پی جویی، شناسایی و تعقیب جرایم یا استفاده غیر از سیستم ارتباطات الکترونیک.

۲-۴-۲- دستورالعمل تجارت الکترونیک ۲۰۰۲[۲۲]

این دستورالعمل اگرچه با تأکید بر تجارت الکترونیک تدوین یافته است اما در سایر موارد نیز در قانونگذاری‌های کشورهای عضو مورد توجه قرار گرفته است و از آنجا که در مورد مسئولیت کیفری ارائه کنندگان خدمات در حالات مختلف، مقرراتی دارد لذا از جهت این بحث حائز اهمیت می‌باشد. بخش اول این دستورالعمل مسئولیت جامعه اطلاعاتی در برابر تجارت الکترونیک می‌باشد و دربردارنده مقرراتی است که برای حقوق کاربران در تجارت الکترونیک بایستی رعایت شود.

بخش دوم- مسئولیت ارائه کنندگان خدمات اینترنتی می‌باشد و با توجه به انواع خدمات ارائه شده در حالات زیر مطرح و مسئولیت آنها تعیین گردیده است:

۱- mere conduit یا صرف انتقال که ارائه کننده خدمات صرفاً انتقال اطلاعات یا دستیابی آن را فراهم نموده است. در این حالت ارائه کننده خدمات برای ورود خسارت یا جبران خسارت یا ضمانت اجرای کیفری ناشی از آن انتقال اصولا مسئولیت ندارد مگر اینکه نسبت به محتوایی که انتقال می‌یابد آگاهی داشته باشد، که در حالات زیر فرض شده است.

الف) انتقال را آغاز کرده باشد.

ب) دریافت کننده انتقال را انتخاب کرده باشد.

ج) محتوای اطلاعات در همان انتقال را انتخاب کرده یا تغییر داده باشد (ماده ۱۷)

۲- caching شامل خدمات ذخیره واسط خودکار و موقت اطلاعات بمنظور تسهیل و تسریع تبادل اطلاعات می‌باشد. در این حالت نیز ارائه کننده خدمات مسئولیت ندارد (اعم از مدنی و کیفری) مگر اینکه:

الف) اطلاعات را تغییر دهد.

ب) شرایط دسترسی در مبدأ اصلی ارائه اطلاعات را نقض کرده باشد.

ج) در صورت تغییر اطلاعات در منبع اصلی، اطلاعات را روزآمد نکند.

د) اگر بداند اطلاعاتی که در منبع اصلی ارائه می‌شود غیر قانونی است یا براساس حکم مقامات قضایی حذف یا غیر قابل دسترس شده یا دستور حذف یا غیر قابل دسترس نمودن آن صادر شده است.

22- The Electronic Commerce (EC Directive) Regulations 2002

۳- Hosting یا واگذار ی فضای لازم برای ذخیره اطلاعات ارائه کننده خدمات میزبانی یا hosting در موارد زیر بموجب ماده ۱۹ مسئولیت دارد.

الف) ارائه کننده خدمات:

۱) اطلاع واقعی از اقدامات یا اطلاعات غیر قانونی نداشته و از قرائن و اوضاع و احوال نیز مشخص نباشد که اطلاعات یا اقدامات غیر قانونی است.

۲) به محض اطلاع یا آگاهی سریعاً برای حذف یا غیر قابل دسترس ساختن اقدام ننماید.

ب) گیرنده خدمات مطابق اختیارات یا نظارت ارائه کننده خدمات اقدام نکرده است.

۳- انجمن بین‌المللی حقوق جزا

انجمن بین‌المللی حقوق جزا سازمان غیر دولتی است که همکاری فعالی با سازمان ملل دارد و مشاور شورای اقتصادی ـ اجتماعی است. این انجمن هر چهار سال یک بار چند موضوع را به عنوان موضوعات مورد بحث مطرح می‌کند و از کشورهای عضو که دارای گروه ملی هستند یا از اعضای خود در کشورهای مختلف می‌خواهد تا با توجه به پلان و پرسش‌نامه تنظیمی، اقدام به ارسال مقالات (تحت عنوان گزارش ملی) بنمایند، طراح پلان و پرسش نامه خود از صاحبنظران آن بحث است.

در سال ۱۹۹۰ یکی از موضوعاتی که انجمن مطرح کرد، جرایم رایانه‌ای و سایر جرایم در قلمرو انفورماتیک بود.[۲۳] در سال ۱۹۹۲ نشست مقدماتی این بحث در دانشگاه ورتسبورگ آلمان انجام شد. همزمان با آن سازمان ملل، جامعه اروپا و شورای اروپا نیز جلسات مشترکی در همین مورد منعقد کردند. نتیجه کار انجمن چاپ کتابی ویژه جرایم رایانه‌ای (جلد ۶۴ شماره ۱,۲ نشریه انجمن) بود.

۳-۱- توصیه‌های کنفرانس انجمن بین‌المللی حقوق جزا (AIDP) در مورد جرایم رایانه‌ای و دیگر جرایم علیه تکنولوژی اطلاعات

در سال ۱۹۹۴ نشست نهایی انجمن در ریودوژانیرو در ۴ الی ۱۰ سپتامبر برگزار شد و توصیه نامه‌ای که حاوی مطالبی در خصوص اقدامات پیشگیرانه غیر کیفری ـ حقوق جزای ماهوی ـ حمایت از حقوق خصوصی و فردی ـ قوانین دادرسی و همکاری‌های بین المللی می‌باشد تصویب نمود، که در ادامه به اهم آن اشاره می‌گردد.

۳-۱-۱- اقدامات پیشگیرانه غیر کیفری

انجمن با تأکید بر اینکه استراتژی کلی پیشگیری و کنترل جرایم انفورماتیک را نمی‌توان به تدابیر قانونی محدود کرد یکسری تدابیر غیر کیفری را پیشنهاد می‌کند از قبیل:

۲۳- طراح پلان و پرسش نام پروفسور اداریش زیر بود، جهت مطالعه متن پرسش نامه می‌توان به مأخذ زیرمراجعه کرد: زیر، اولدیش «جرائم رایانه‌ای و دیگر جرائم مرتبط با تکنولوژی اطلاعات» ترجمه محمدحسن دزیانی ـ گزارش رایانه ـ شماره ۱۲۲- ۱۳۷۲

- استفاده از تدابیر امنیتی داوطلبانه بوسیله استفاده کنندگان از رایانهها،
- اجباری کردن اعمال تدابیر امنیتی در بخشهای حساس،
- وضع قوانین و اتخاذ تدابیر اجرایی ـ اداری برای ارتقاء امنیت رایانه به وسیله حکومت‌های ملی
- ارائه دستورالعمل، تشریح و ارتقای اقدامات امنیتی بوسیله صنعت تکنولوژی اطلاعات
- گسترش و ارتقای اصول اخلاق انفورماتیک بوسیله بخشهای مختلف جامعه بویژه از طریق مؤسسات آموزشی، تشکیلات حرفه‌ای و مردم.
- ارتقای همکاری بزهدیده در افشای جرمهای رایانه‌ای
- تربیت و آموزش پلیس و برگزاری دوره‌های تخصصی برای قضات ویژه رسیدگی به این قبیل جرایم.

۲-۱-۳- حقوق جزای ماهوی

انجمن با بیان اینکه سوء آستفاده از تکنولوژی اطلاعاتی به منافع اقتصادی اطلاعات و منافع فردی به یک میزان مربوط می‌شود اشاره می‌کند که استفاده غیر قانونی از پردازش انفورماتیک ممکن است بوسیله تجاوز به ارزشهای سنتی به کار گرفته شود که در اینجا خلاء های حقوق جزای سنتی آشکار می‌شود و به علاوه ممکن است گسترش تکنولوژی اطلاعات ارزش‌ها و منافع جدیدی را به وجود آورد که به حمایت قانونی نیاز دارد از جمله تمامیت سیستم‌های اطلاعات و داده‌های آن و نیز امنیت و انحصاری بودن برخی از داده‌ها، لذا اصلاح قوانین کیفری یا وضع طبقه‌بندی‌های جدید جرایم باید اتخاذ شود.

در خصوص انواع جریم، انجمن یا پذیرش خطوط راهنمای پیشنهادی به قانونگذاران ملی در توصیه‌نامه شماره ۹ R(۸۹) شورای اروپا و تقسیم‌بندی آن، نظر به پیشرفت تکنولوژی اطلاعات و افزایش جرایم مربوط به آن از زمان تصویب توصیه‌نامه فوق (۱۹۸۹) و با توجه به ارزش قابل توجه ثروتهای غیرمادی در عصر اطلاعات توصیه می‌کند که علاوه بر فهرست اجباری جرائم در توصیه‌نامه شورای اروپا موارد مذکور در فهرست اختیاری بویژه تغییر داده‌ها و اطلاعات و جاسوسی آمریکا را نیز جرم‌انگاری نمایند و همچنین جرایم زیر نیز به عنوان جرایمی مستقل منظور شوند.

الف) قاچاق کلمات رمز

ب) انتشار ویروس یا برنامه‌ای مشابه

ج) دستیابی به اسرار برخلاف قانون

د) به‌کارگیری، انتقال و دگرگونی غیر قانونی داده‌های شخصی

انجمن همچنین توصیه می‌کند برای جلوگیری از تورم کیفری باید جرایم رایانه‌ای به اعمال عمدی محدود شوند و با تأکید بر اینکه در عصر اطلاعات در حال انتقال حمایت از زندگی خصوصی فردی در برابر خطرهای ناشی از تکنولوژی انفورماتیک باید به رسمیت شناخته شود. با وجود این منافع مشروع گردش آزاد اطلاعات باید محترم شمرده شود. استفاده از مقررات جزایی برای حمایت از حقوق خصوصی و فردی را تنها جایی مجاز می‌داند که از طریق مقررات مدنی و اداری حمایت مناسب برقرار نگردد.

۳-۱-۳- قوانین دادرسی و همکاری بین‌المللی

انجمن در خصوص قوانین دادرسی به لزوم اختیارات کامل مقامات مسئول تحقیق و تعقیب جرائم رایانه‌ای را که با مقررات صریح و مطابق اصول و قوانین بین‌المللی حقوق بشر از هرگونه سوء استفاده جلوگیری نماید، پیشنهاد می‌کند. همچنین تغییرات

مناسب قوانین درمورد قابل قبول بودن قرائن در محیطهای رایانه‌ای و نیز در نظر گرفت خسارات وارده به ارزشهای پیرامون تکنولوژی مثل از دست دادن یک فرصت اقتصادی ـ تجاوز به زندگی ـ بهای بازسازی داده ها و ... را لازم می‌داند.

بلحاظ قابلیت نقل و انتقال داده‌های رایانه‌ای در سیستم‌های ارتباط از راه دور بین‌المللی و طبیعت کاملاً بهم پیوسته جامعه اطلاعاتی مدرن، همکاری بین‌المللی برای پیش‌گیری و تعقیب جرایم بسیار حیاتی و گسترش همکاری در زمینه‌های ذیل را لازم می‌داند.

- امنیت سیستم‌های رایانه‌ای
- حل مسایل مربوط به صلاحیت قضایی
- توافق‌های بین‌المللی برای تحقیق و تعقیب فرامرزی قانونی، مؤثر و فوری در مورد سیستم‌های رایانه‌ای به هم پیوسته.

٤- اقدامات سازمان ملل متحد

جرم رایانه‌ای شکل تازه‌ای از جرایم فراملی است و محدوده بالقوه آن به همان گستردگی سیستم‌های ارتباطی بین‌المللی می‌باشد و برای مبارزه با آن باید تمامی مناطق جهان سهیم باشند. و مبارزه مؤثر نیازمند اتفاق نظر جهانی در مورد ماهیت و نوع این جرایم و راه‌حل‌های ممکن، وجود هماهنگی در قوانین آیین دادرسی کشورها و همکاری بین‌المللی است. در حالیکه عمده اقدامات در این راستا در کشورهای اروپایی و سازمان‌های منطقه‌ای آنان تمرکز یافته است. سازمان ملل بعنوان یک سازمان بین‌المللی سهم عمده‌ای در این راستا می‌تواند داشته باشد. کما اینکه از دهۀ هشتاد این امر مورد توجه سازمان بوده است و کنگره سازمان ملل متحد درباره پیش‌گیری از جرم و درمان مجرمان، در این خصوص قطعنامه‌ها و توصیه‌نامه‌های متعدد داشته است.

نخستین بار پس از برگزاری هفتمین کنگره سازمان ملل متحد درباره پیشگیری از جرم و درمان مجرمان که درسال ۱۹۸۵ برگزار شد، دبیر کل سازمان گزارشی تحت عنوان «پیشنهادهایی برای اقدامات هماهنگ بین‌المللی علیه اشکال به رسمیت شناخته شدۀ جرایم در طرح اجرایی میلان» (E/AC . ۵۷/۱۹۸۸/۱۶) ارائه داد که در پاراگراف‌های ۴۲ تا ۴۴ آن گزارش، به جرایم رایانه‌ای مورد بحث قرار گرفت.

متعاقباً این موضوع در دستور کار کنگره هشتم قرار گرفت و از آن زمان به بعد بموجب قطعنامه کنگره هشتم کمیته پیش‌گیری و کنترل جرم عهده‌دار سازمان دهی کوشش‌های بین‌المللی برای ارتقاء و تعمیم چارچوب جامع از خطوط راهنما و استانداردهایی شود که به دولتهای عضو در برخورد با جرایم رایانه‌ای کمک کند.

٤-١- دستاوردهای کنگره هشتم پیشگیری از جرم و درمان مجرمان

در برنامه‌های تدارکاتی هشتمین کنگره سازمان ملل متحد درباره جلوگیری از حرم و درمان مجرمان، اجلاس مقدماتی منطقه‌ای آسیا و اقیانوس آرام، نگرانی خود را درباره آثار پیشرفتهای تکنولوژی و انعکاس آن در جرایم رایانه‌ای اعلام داشت.[۲۴] در اجلاس مقدماتی منطقه‌ای اروپا پیشنهاد شد که مبارزه بین‌المللی با جرایم رایانه‌ای باید از سوی هشتمین کنگره سازمان ملل متحد و کنگره‌های پس از آن مورد حمایت و توجه قرار گیرد.[۲۵]

24- A/ CONF.144/RPM.1
25- A/ CONF. 144/RPM.2

در کنگره هشتم که در هاوانا از ۲۷ اوت تا ۷ سپتامبر ۱۹۹۰ تشکیل شد، نهایتاً در دوازدهمین اجلاس عمومی آن پیش‌نویس قطعنامه‌ای توسط نماینده کانادا که از طرف ۲۱ عضو حامی امضاء شده بود در مورد جرایم رایانه‌ای تسلیم کنگره شد. که در سیزدهمین اجلاس قطعنامه مورد پذیرش قرار گرفت و مجمع عمومی نیز در قطعنامه ۴۵/۱۲۱ خود اسناد و قطعنامه‌های مصوب هشتمین کنگره را پذیرفت و از دولت‌ها خواست تا در تبیین قوانین و دستور العمل‌های تعیین کننده خط مشی خود و براساس شرایط اقتصادی، اجتماعی، حقوقی، فرهنگی و سیاسی هر کشور از قطعنامه تبعیت کنند. در این قطعنامه از کشورهای عضو خواسته شده است که در صورت لزوم با مدنظر قرار دادن موارد زیر تلاش‌های خود در مبارزه با جرایم رایانه‌ای شدت بخشند:

الف) مدرنیزه کردن قوانین و دادرسی‌های کیفری ملی شامل این موارد:

۱) حصول اطمینان از این که جرایم و قوانین موجود مربوط به نیروهای تحقیقات (جنایی) و قابلیت پذیرش ادله در دادرسی‌های قضایی به اندازه کافی قابل اعمال است و در صورت لزوم تغییرات مقتضی اعمال می‌شود.

۲) در صورت نبود قوانین کافی و در موارد نیاز، جرایم و تحقیقات و دادرسی‌های مستند به ادله ایجاد شود که پاسخگوی این شکل پیچیده و نوین فعالیت‌های مجرمانه باشد.

۳) فراهم ساختن امکان ضبط یا استرداد وجوه (و مزایای) به دست آمده از روش های غیر قانونی و ناشی از ارتکاب جرایم مربوط به رایانه.

ب) ارتقای ضوابط پیش‌گیرانه و امنیتی رایانه، با توجه به مسایل مربوط به حمایت از حقوق خصوصی، احترام گذاردن به حقوق بشر و آزادی‌های اساسی او و هرگونه مکانیزم تنظیم مقررات مربوط به استفاده از رایانه.

ج) گزینش راه‌هایی برای حساس کردن عامه مردم و قوه قضائیه و عاملان اجرای قوانین نسبت به این مسئله و اهمیت جلوگیری از ارتکاب جرایم رایانه‌ای.

د) دادن آموزش کافی به قضات، مأموران و عوامل مسؤول در زمینه جلوگیری، تحقیقات تعقیب و احقاق حق در جرایم اقتصادی و رایانه‌ای.

ه) مطالعات دقیق با همکاری سازمان‌های ذینفع در مورد قواعد اخلاقی مربوط به استفاده از رایانهها و تعمیم این قواعد به عنوان بخشی از مواد درسی و آموزشی انفورماتیک.

د) اتخاذ سیاست‌های مربوط به بزهدیدگان جرایم رایانه‌ای براساس اعلامیه سازمان ملل متحد و در مورد اصل بنیادین عدالت برای بزهدیدگان جرایم و سوءاستفاده از قدرت، شامل استرداد دارایی که به‌طور غیر قانونی کسب شده است و تشویق بزهدیدگان به گزارش اینگونه جرایم به مقامات صالحه.

همچنین به کنگره هشتم در قطعنامه خود پیشنهاد کرد که کمیته جلوگیری و کنترل جرایم، باید برای پیشبرد تلاش‌های بین‌المللی به‌منظور توسعه و ترویج چارچوب جامعی که به کشورهای عضو در مبارزه با جرایم رایانه‌ای یاری دهد. و نیز پیشنهاد شد این مسایل به وسیله اجلاس ویژه کارشناسان مورد بررسی قرار گیرد و از دبیر کل خواسته شد تا انتشار یک کتابچه فنی در خصوص جلوگیری و تعقیب چنین جرایمی را عهده‌دار شود. در حدود چارچوب این قطعنامه دولت کانادا برای ارائه این کتابچه فعالیت‌هایی انجام داد و در گردهمایی متخصصان در خصوص جرم رایانه‌ای و دیگر جرایم علیه تکنولوژی اطلاعات در اکتبر ۱۹۹۲ در ورتسبورگ مورد تجدیدنظر قرار گرفت و نتیجه آن در شماره‌های ۴۳ و ۴۴ نشریه بین‌المللی سیاست جنایی ارائه

گردید.[۲۶] لازم به ذکر است گردهمایی ورتسبورگ به وسیله انجمن بین‌المللی حقوق جزا منعقد شد و سازمان ملل و شورای اروپا و اتحادیه اروپا مشترکاً در آن شرکت کردند.

کتابچه موجب تغییر رهیافت سازمان ملل در خصوص پیش‌گیری از جرم و برنامه عدالت کیفری برای مسئله کنترل جرم شده است که بوسیله قطعنامه ۴۶/۱۵۲ مجمع عمومی سازمان و قطعنامه ۱۹۹۲/۲۲ شورای اقتصادی و اجتماعی توجه شده است. این رهیافت فنی در کتابی تحت عنوان «راهنما برای رایانه‌ای کردن سیستم‌های اطلاعاتی و عدالت کیفری» منتشر شد و به طور وسیع استفاده کافی از رایانهها در سیستم مدیریتی عدالت کیفری را پیشنهاد کرده است.

این کتابچه حاوی مطالبی در خصوص پدیده جرم رایانه‌ای (تعریف و پدیده شناسی و انواع آن) . حمایت حقوق ماهوی از مالک داده‌ها و اطلاعات ـ حمایت حقوق جزای ماهوی از حقوق خصوصی و فردی آیین دادرسی کیفری و جلوگیری از ارتکاب جرایم در محیط رایانه‌ای می‌باشد.

در خصوص انواع جرایم رایانه‌ای سازمان ملل با تأکید بر تقسیم‌بندی های OECD و شورای اروپا به انواع مشترک و عمومی جرایم رایانه‌ای اشاره می‌کند که شامل:

- کلاهبرداری با سوء استفاده از رایانه
- جعل رایانه‌ای
- ایجاد خسارت (تخریب) یا تغییر در داده‌ها یا برنامه‌های رایانه‌ای
- دستیابی غیر مجاز به سیستمها و خدمات رایانه‌ای
- تکثیر غیر مجاز برنامه‌های رایانه‌ای قانوناً حمایت شده

۲-٤- کنگره نهم و جرایم رایانه‌ای از منظر جرایم سازمان یافته فراملی

با پیشرفت تکنولوژی رایانه و مخابرات و توسعه فزاینده شبکه‌های ارتباطی در سطح دنیا و همچنین امکان سوء استفاده مجرمین از این شبکه‌ها در ارتکاب جرایم نخستین بار بحث شبکه‌های رایانه‌ای و اینترنت بعنوان ابزار کار مجرمین درکنگره نهم مورد توجه قرار گرفت.[۲۷] البته در این کنگره جرایم رایانه‌ای عنوان مستقل نداشته و در گروه جرم سازمان یافته فراملی تحت عنوان چالشهای جرم فراملی و ارتشاء مورد توجه قرار گرفت (بند ۶). و نهایتاً موضوع تبادل اطلاعات بین کشورها و تحولات تکنیک‌های جدید همکاری بین کشورها در خصوص جرائم سازمان یافته فراملی مطرح و توصیه‌هایی در خصوص این جرائم شده که شامل جرایم رایانه‌ای فراملی که به صورت سازمان یافته انجام می‌شوند نیز می‌گردد و تأکید بر پرنوگرافی کودک و اشکال استثمار بزهدیدگان بوده است.[۲۸]

«پورنوگرافی کودک» در پروتکل اختیاری کنوانسیون حقوق کودک دربارهٔ فروش کودک، فحشای کودکان و پرنوگرافی کودک ۲۵ / مه/ ۲۰۰۰ ، بدین صورت تعریف شده است: «هر نمایش به هر طریق و وسیله از یک کودک تحریک و تشویق شده در فعالیتهای جنسی صریح واقعی یا شبیه سازی شده یا هرگونه نمایش قسمت‌های جنسی یک کودک برای هدف‌های بدواً

۲۶- این نشریه توسط اقای محمدحسن دزیانی و آقای مهندس حیام روحانی ترجمه و در جلد اول «جرایم رایانه‌ای»، دبیرخانه شورای عالی انفورماتیک – سازمان برنامه و بودجه درج شده است.

27- E / CN.15 / 2000/ 2

28- Report of the execution Director challenge of transational crime and corruption.

جنسی» . در گذشته پورنوگرافی کودک به شکل‌های کاغذی، ویدئو و نقاشی داشته، با ورود اینترنت و در ارتباط با پیشرفت‌های تکنولوژیک، تغییر زیادی در حجم و ماهیت قابلیت دسترسی به پورنوگرافی کودک ایجاد شده است. اینترنت نه تنها به عنوان یک مکانیسم برای ایجاد، تجارت و توزیع پورنوگرافی کودک عمل می‌کند بلکه همچنین به عنوان یک وسیله برای مرتکبین پورنوگرافی کودک جهت ایجاد ارتباط و جذب بزهدیدگان جدید عمل می‌نماید. اغلب و در عمل سوءاستفاده‌کنندگان جنسی کودک حلقه وسیعی را تشکیل می‌دهند که به تولید و توزیع پورنوگرافی کودک اقدام می‌کنند.

کنوانسیون مبارزه با جنایات سازمان یافته (معروف به کنوانسیون پالرمو) در ۱۵ / نوامبر/ ۲۰۰۰ با تصویب قطعنامه ۵۵/۳۸۳ توسط مجمع عمومی سازمان ملی پذیرفته شده است.[۲۹]

۳-٤- کنگره دهم و توجه به اشکال جدید جرایم رایانه‌ای و تکنولوژی‌های برتر

قبلی از تشکیل کنگره دهم کمیسیون پیشگیری از جرم و عدالت کیفری[۳۰] تصمیم گرفت ۴ کارگاه در کنگره دهم خواهند بود که یکی از آنها در مورد «جرایم مرتبط با شبکه رایانه‌ای» است.

مجمع عمومی سازمان ملل در قطعنامه ۵۲/۹۱ از۱۲ دسامبر ۱۹۹۷ و ۵۳/۱۱۰ از ۹ دسامبر ۱۹۹۸ در مورد تدارک برای دهمین کنگره پیشگیری از جرم و درمان مجرمان که بوسیله شورای اجتماعی و اقتصادی بعد از ششمین و هفتمین کمیسیون در مورد پیشگیری از جرم و عدالت کیفری، پیشنهاد شده بود، تصمیم گرفت به ۴ موضوع درکنگره دهم پرداخت شود و کارگاه‌های تخصصی آن تشکیل گردد که یکی از آنها «جرایم مرتبط با شبکه رایانه‌ای» " Crime Related of computer Network" بود.

در دومین نشست متخصصین در مورد جرایم مرتبط با شبکه رایانه‌ای مؤسسه آسیا و خاور دور سازمان ملل برای پیشگیری از جرم و اصلاح و درمان مجرمان (UNAFEI) که در اکتبر ۱۹۹۹ تشکیل گردید و موضوعات مورد توجه آن اشکال مختلف جرائم که در نشست نخست بررسی شده بود از جمله اعمال مجرمانه علیه کارکرد سیستم‌های رایانه‌ای و داده‌هایی که در آن سیستم‌ها هستند، شامل دستیابی غیر مجاز به سیستم‌ها و داده‌ها و اهمیت شبکه‌های محلی و شبکه‌های بین‌المللی برای ارتکاب دیگر جرایم، استفاده از شبکه‌های رایانه‌ای (که لزوماً بطور مستقیم علیه سیستمها یا داده‌های رایانه‌ای نیستند مانند محتوای مربوط به پورنوگرافی اطفال) (Computer-related crime) می‌توان قرار داد. و بویژه تأکید بر روی ابزارهای تحقیقات لازم برای جمع‌آوری ادله که برای مبارزه با جرایم مرتبط با رایانه ضروری هستند و همچنین با تأکید بر اطلاعات عملی و فنی که برای تحقیقات و تعقیب این جرایم لازم هستند.[۳۱]

نهایتاً در قطعنامه کنگره دهم[۳۲] صراحتاً تحت عنوان computer related crime به موضوعات مختلف پیرامون پیشگیری و مبارزه با جرایم رایانه‌ای اشاره شده است. و حاوی موارد ذیل می‌باشد,

---

29- United nations convention against transnational organized crime . united nations / 2000
30- Commission on crime prevention and criminal Justice
31- Report of the "2nd EXPERTS MEETING ON CRIME RELATED TO THE COMPUTER NETWORK UNITED NATION... Asia and for East Institute for the prevention of crime and the treatment of offenders (UNAFEI)" 25-28 october 1999
32- E/CN. 15/2001/4-2001/ /30

۱- مقدمه
۲- پیشینه که حاوی ۴ عنوان است: الف) فعالیت‌های بین حکومتی و یا سازمان‌های بین‌المللی
ب) فعالیتهای سازمان ملل
ج) ماهیت و تیپ شناسایی جرایم رایانه‌ای و تکنولوژی برتر
د) ارزیابی محدوده و هزینه‌های رایانه‌ای و تکنولوژی برتر
۳- جمع‌بندی و توصیه‌ها که با تأکید بر مسائل پیشگیری و کنترل جرم شامل موارد ذیل می‌باشد.
الف) نیاز به بحث جرم رایانه‌ای و تکنولوژی برتر بعنوان یک موضوع داخلی
ب) لزوم کمک به کمک کشورهای در حال توسعه
ج) نیاز به ملاحظات بین‌المللی یا اتخاذ تدابیر بین‌المللی ملی و بخش خصوصی
د) نقش سازمان ملل
ه) عناصر و اجزاء یک مطالعه مفصل
ز) اختیارات و توصیه‌های خاصی برای آینده

که در ادامه با توجه به طبقه‌بندی و تیپ‌شناسی که در این قطعنامه از جرایم رایانه‌ای شده است و لحاظ اشکال جدید مجرمانه در آن و سپس توصیه‌های خاصی برای آینده بیان می‌گردد.

۱-۳-۴- انواع جرایم رایانه‌ای و جرایم تکنولوژی برتر

در قطعنامه سه دسته جرایم از یکدیگر مجزا شده‌اند که شامل:

دسته اول ـ جرایم ارتکابی علیه تکنولوژی‌ها و کاربران آنها

الف) دستیابی غیر مجاز به رایانه یا سیستم های رایانه‌ای
ب) استفاده غیر مجاز از سیستم‌های رایانه‌ای
ج) خواندن، کپی کردن یا گرفتن داده بدون اجازه
د) ایجاد یا تمهید برنامه‌های مهاجم
ه) تخریب داده‌ها و سیستم‌های رایانه‌ای مورد استفاده عموم[۳۳] و سابوتاژ رایانه‌ای

دسته دوم: جرایم سنتی با استفاده از رایانه یا تکنولوژی‌های ارتباطی

الف) جرایم مربوط به محتوای مجرمانه
ب) کودک‌ربایی اینترنتی (بمنظور سوء استفاده جنسی)
ج) کلاه‌برداری
د) جاسوسی صنعتی یا تجاری
ه) جرایم مالکیت فکری
و) قاچاق
ز) پول‌شویی

33- Vandelism

دسته سوم – استفاده از تکنولوژی برای حمایت از فعالیت‌های مجرمانه دیگر

استفاده از تکنولوژی باعث می‌شود مرتکب در پوشش یک شغل مشروع ظاهر شده و به‌طور ناشناس با هزینه کم و در سطح جهانی اقدام به فعالیت مجرمانه نماید و یا از تکنولوژی شبکه برای حمایت از اشکال جدید جرایم و سازمان‌های مجرمانه از قبیل (syber drage) قاچاق مواد روان‌گردان، استفاده نماید.

۲-۳-۴- اختیارات و توصیه‌های خاص برای آینده

در این بخش امکان یک سند بین‌المللی علیه جرم رایانه‌ای و تکنولوژی‌های برتر مورد بررسی قرار گرفته است و توصیه شده که گروه‌های متخصص به مشاوره درباره این مسائل بپردازند و مطالعات عملی و ملموس انجام داده و پیش نویس طرحی را بعنوان یک سند بین‌المللی علیه جرم رایانه‌ای و تکنولوژی برتر تهیه نمایند. همچنین در خصوص تهیه این سند بین‌المللی مسائل اساسی که باید مدنظر قرار گیرد توجه داده شده است از جمله:

الف) این سند باید قواعد را بیان کند[۳۴] یا الزام‌آور باشد[۳۵].

به عبارتی آیا این سند یکسری خطوط راهنما برای کمک به دولتها برای گسترش تدابیر داخلی باید باشد یا خیر جنبه الزام‌آور داشته باشد؟ و چه اقداماتی را باید دربرگیرد و چگونه حقوق و آیین دادرسی استاندارد شود؟

ب) چه ارتباطی باید بین این با سند کنوانسیون مبارزه با جرایم سازمان یافته فراملی وجود داشته باشد؟

ج) اطمینان از چارچوبها به نحویکه تمامیت سیستم‌های داخلی و بین‌المللی به گونه‌ای رعایت شود که با تغییرات جدید هماهنگ باشد. به عبارتی در زمان طراحی و نوشتن پیش‌نویس توصیه شده به عنوان تکنولوژی خنثی نوشته شود.

د) در ملاحظات حریم خصوصی آزادی بیان و دیگر حقوق بشر مدنظر قرار گیرد (در ابزارهای لازم برای پیشگیری و کنترل جرم)

ملاحظه می‌گردد اشکال جدید سوءاستفاده‌ها از رایانه و تکنولوژی های جدید مدنظر بوده است و توسعه این تکنولوژی و ظهور اشکال سازمان یافته و فراملی این جرایم و همچنین مبارزه مؤثر علیه این جرایم ضرورت یک سندو ابزار بین‌المللی را بیشتر از بیش آشکار نموده که مورد توجه سازمان ملل قرار گرفته است. که البته با توجه به سطح متفاوت تکنولوژی تفاوت‌های اساسی در سیستم‌های حقوقی کشورها و ارتباط بسیاری از این مواد با مسائل اقتصادی و بعضاً سیاسی مسلماً حصول به یک سند بین‌المللی را با دشواری هایی مواجه خواهد ساخت.

کنگره یازدهم – انعکاس قطعنامه کنگره نهم در سطح کشورها

در سند کنگره یازدهم (E/CN,15/2002/8) – ۲۹ ژانویه ۲۰۰۲ – در خصوص جرایم مرتبط با رایانه پیشرفتهای اخیر در خصوص مبارزه با این جرایم منعکس شده است که شامل:

34- Normative
35- binding

- وضعیت کوشش‌هایی که برای پیشگیری و کنترل جرایم رایانه‌ای شده است.
- پیشرفت‌های کشورها در سایه قطعنامه سازمان ملل مورد بررسی قرار گرفته است و
- تهدیدات ناشی از این جرایم بویژه افزایش استفاده از رایانه توسط گروه‌های مجرمانه سازمان یافته مورد توجه قرار گرفته
- پیشرفت‌های اینترپول یا واحدهای دیگر پلیس در مبارزه با این جرایم و اقدامات شورای اروپا نیز اشاره شده است.

۵- اقدامات پلیس بین‌الملل در مبارزه با جرایم رایانه‌ای

سالهاست که اینترپول در مبارزه با جرایم مرتبط با فناوری اطلاعات فعال می‌باشد. این سازمان با بهره‌گیری از کارشناسان و متخصصین کشورهای عضو اقدام به تشکیل گروه‌های کاری در این زمینه کرده است. رؤسای واحدهای مبارزه با جرایم رایانه‌ای کشورهای با تجربه عضو سازمان در این گروه کاری گرد هم آمده‌آند گروه‌های کاری منطقه‌ای در اروپا، آسیا، آمریکا و آفریقا مشغول بکارند و زیر نظر کمیته راهبردی جرایم فن‌آوری اطلاعات، مستقر در دبیرخانه کل اینترپول فعالیت می‌نمایند.[۳۶]

۵-۱- گروه‌های کار منطقه‌ای اینترپول

گروه کار اروپایی اینترپول با حضور کارشناسان هلند، اسپانیا، بلژیک، فنلاند، فرانسه، آلمان، ایتالیا، سوئد و انگلیس در سال ۱۹۹۰ تشکیل شد این گروه هر سال ۳ بار تشکیل جلسه می‌دهد. تهیه کتابچه راهنمای پی‌جویی جرایم رایانه‌ای، کتاب و سی‌دی راهنمای جرایم رایانه‌ای تشکیل دوره‌های آموزشی برای نیروهای پلیس، تشکیل سیستم اعلام خطر که مرکب از: سیستم‌های پاسخگویی شبانه‌روزی، نقاط تماس دایمی شبانه‌روزی، تبادل پیام بین‌المللی در قالب فرمهای استاندارد در زمینه جرایم رایانه‌ای و انجام چندین پروژه تحقیقاتی پیرامون موضوعات مرتبط با جرایم کامپیوتری از جمله اقدامات گروه کاری مذکور می‌باشد.

گروه کاری آمریکایی جرایم مرتبط با تکنولوژی اطلاعات مرکب از کارشناسان و متخصصین پلیس کشورهای کانادا، ایالات متحده آرژانتین، شیلی، کلمبیا، جامانیکا و باهاما است.

گروه کار افریقایی جرایم مرتبط با تکنولوژی اطلاعات مرکب از کارشناسان آفریقای جنوبی زیمباوه، نامبیا، تانزانیا، اوگاندا، بوتسوانا، سوازیلند، زنگبار، سوتو و رواندا در ژوئن ۱۹۹۸ تشکیل گردید. آنها کارشان را با برگزاری یک دوره آموزشی آغاز نمودند و دومین دوره آموزشی آنها با مساعدت‌های سفارتخانه‌های انگلیس و فرانسه برگزار شد.

گروه کاری جنوب اقیانوس آرام و آسیا در نوامبر ۲۰۰۰ در هند تشکیل شد و کارشناسانی از کشورهای استرالیا ـ هنگ کنگ ـ هند ـ ژاپن ـ نپال و سریلانکا عضو آن هستند این گروه کاری با الگو قرار دادن کمیته راهبردی جرایم مربوط به فن‌آوری اطلاعات به منظور ایجاد و هماهنگی میان اقدامات گروه‌های کاری منطقه‌ای در محل دبیرخانه کل اینترپول تشکیل گردیده است.

۳۶- رضا پرویزی، مجموعه مقالات اولین همایش تخصصی بررسی جرایم رایانه‌ای – ۱۳۸۰/۱۰/۲۲

۲-۵- اولین کنفرانس بین‌المللی جرم رایانه‌ای (لیون ۱۹ و ۲۰ آوریل ۱۹۹۵)

این کنفرانس که در تاریخ فوق با حضور نمایندگان پلیس بین‌الملل دولتها تشکیل گردید و مسائل مربوط به طرق ارتکاب جرایم رایانه‌ای و تکنولوژیهای در اختیار برای کشف و پی جویی و جمع‌آوری ادله در این جرائم و قوانین موجود مورد بررسی قرار گرفت و نهایتاً توصیه‌نامه‌ای را به شرح ذیل به تصویب رساند.

در این توصیه‌نامه با توجه به اهمیت فزاینده استفاده و سوءاستفاده از رایانه در همه انواع جرم، و با در نظر گرفتن کارهای انجام شده از سوی پلیس بین‌الملل بویژه:

۱) برقراری نقاط ارجاع مرکزی ملی و اجرا و بکارگیری پیام جرم رایانه‌ای برای انجام تبادل سریع اطلاعات در موارد مزبور،

۲) انتشار کتابی در زمینه رایانهها و جرم و ارائه کتابچه جامع جرم رایانه‌ای در آینده نزدیک

۳) آماده کردن رشته‌های آموزشی برای تحقیق‌کنندگان پلیس توسط سازمان اینترپول توصیه می‌کند که:

۱) مشکل جرم رایانه‌ای باید به‌طور مشابه در هر یک از کشورهای عضو اینترپول و در مناطق آمریکایی، آفریقایی و آسیایی با احتمال معاضدت تکنیکی برای این مناطق از طریق دبیر کل در نظر گرفته شود.

۲) یک کمیته راهنما برای اقدام و همکاری در اقدامات منطقه‌ای و تشویق عمومی وحدت روش‌ها و رویه‌های مورد توافق در تحقیقات (جنایی) رایانه‌ای بین‌المللی تشکیل شود.

۳-۵- راهنمای جرایم رایانه‌ای ۲۰۰۱

پلیس بین‌الملل در کنار ایجاد پایگاه‌های داده‌ای بزرگ و مفصل حاوی اطلاعات بسیار سودمند از مجرمین و جرایم بالاخص جرایم رایانه‌ای و جرایم مرتبط با آن می‌باشد، اقدام به انتشار راهنماها و منابع آموزشی و فنی برای پلیس و مراجع ذیربط نموده است.

راهنمای جرایم رایانه‌ای ۲۰۰۱ توسط گروه کاری اروپایی جرم رایانه‌ای نگارش یافته و بخشهای متنوع آن شامل توصیفها ـ فورم پیام، جزئیات دوره‌های آموزش‌های اینترپول، قوانین و تکنیک‌های پی‌جویی را، به عنوان یک مرجع جامع برای پی‌جویی‌ها ارائه می‌کند.

در این راهنما با توجه به شبکه‌های مخابراتی و ارتباطی جهانی امروزه، بسیاری جرایم رایانه‌ای هم از حیث وسعت و هم منشاء پدیده‌ای بین‌المللی شده‌اند، بنابراین برای ایجاد و استقرار استانداردهای پی‌جویی فنی و تکنیکی باید کوششی که متمرکز بر تبادل اطلاعات بین کشورها باشد، انجام شود. و بمنظور ایجاد هماهنگی و تسریع در اقدامات پلیس بین‌الملل در بخش جرائم انواع جرایم رایانه‌ای را در هفت دسته برشمرده است و برای هر یک کد ویژه‌ای منظور داشته است، تا در پیام جرم رایانه‌ای بین واحدهای پلیس بین‌الملل استفاده شود. کشورها باید نقاط تماس بین‌المللی به صورت ۲۴ ساعته فعال در دفاتر اینترپول برای مبادله پیام‌های مربوط به جرایم رایانه‌ای ایجاد نمایند.

در بخش دیگری از این راهنما فرم پیام جرم رایانه‌ای ارائه شده است تا در سراسر دنیا بصورت یکسان مبادله شوند. همچنین آدرس‌های نقاط تماس بین‌المللی کشورها در صفحه راهنما ارائه شده است.

٤-٥- نمونه یک عملیات پلیس بین‌الملل

عملیات کاشورال، در آوریل ۱۹۹۶، از کالیفرنیای آمریکا شروع و به سرعت تبدیل به بزرگ‌ترین عملیات در تاریخ پلیس بین‌الملل شد.

شخصی به نام R به اتهام آزار رسانی به یک کودک دستگیر و سپس پلیس دریافت که از دختر ۱۰ ساله دیگری که همکلاس دخترش بوده است نیز سوء استفاده نموده و بطور زنده از طریق دوربین متصل به رایانهش تصاویر آن را روی شبکه می‌گذارد و اعضای دیگر گروه موسوم به کلوپ ارکیده تصاویر را دریافت می‌کنند. این تصاویر در رایانه R ذخیره شده بود و بعداً با استفاده از آنها در اتاق‌های گفت‌و گوی اینترنتی به داد و ستد می‌پرداخت. وی به ۱۰ سال زندان به خاطر جرم ارتکابی و ۱۲ نفر دیگر در بخشهای آمریکا به خاطر عضویت در کلوپ ارکیده به مجازات حبس محکوم شدند.

رایانه R ارتباط سه مورد در بریتانیا را نشان داد که یکی از آنها B یک مشاور رایانه مقیم ساکس بود، پلیس ساکس متوجه ادله دایر بر وجود کلوپ بزرگتری با ۱۸۰ عضو همه نقاط دنیا شد که کلوپ سرزمین عجایب نام داشت. این کلوپ خیلی دقیق و شدید سازمان‌دهی شده بود و دارای یک رئیس، یک دبیر، یک کمیته مدیریت و یک مأمور برای جذب اعضای جدید و ۵ سطح امنیتی برای مخفی ماندن فعالیت‌هایشان از چشم مجریان قانون بود و استفاده زیادی از گذر واژه‌های، ترکیبی و پیچیده و تکنولوژی رمزنگاری می کرد به نحویکه بعضی رایانه‌ها که در این پرونده توقیف شد پلیس و دادگاه هرگز نتوانست آنها را رمزگشایی کند.

از این اعضاء بالغ بر ۷۵۰ هزار تصویر پونوگرافی کرد و ۱۸۰۰ ساعت ویدئویی دیجیتالی سوء استفاده جنسی کودک کشف شد. این افراد غالباً افرادی تحصیل کرده، کارمند و دارای تخصص بالا بودند.

اینترپول موافقت کرد که یگان جرایم ملی انگلیس و پلیس آن کشور با دیگر نیروهای پلیس در سایر کشورها همکاری کنند. و متعاقب آن مظنون‌هایی از ۴۹ کشور شناسایی شدند. توافق شد که نیروهای پلیس به طور هماهنگ به آدرس‌های مظنونین مراجعه کنند تا این افراد نتوانند فرصت آگاه‌سازی سایر اعضای کلوپ و نابودی ادله را پیدا کند. زمان ساعت ۴ به وقت گرینویچ دوم سپتامبر ۱۹۹۸ تعیین شد در کشورهای لهستان و کانادا عملیات سر موقع و باقی کشورها حداکثر با ۱۳ دقیقه تأخیر شروع شد. (سایر کشورها: استرا لیا، بلژیک، انگلیس و ولز، فنلاند ، فرانسه، آلمان، ایتالیا، نروژ، پرتغال. اسکاتلند، سوئد و آمریکا) بودند پلیس هلند بعداً عملیات را انجام داد. مجموعاً ۱۰۵ حکم تفتیش صادر شد و ۱۷ نفر جلب شدند.

البته نتایج بدست آمده از اقدام قوه قضائیه متنوع و جا لب بود. مجازات‌ها از تنوع زیادی برخوردار بود و حتی ادله اثبات بسته به کشور مربوط فرق می‌کرد.

به زعم پلیس بین الملل دلیل عدم شرکت نیروهای پلیس در بعضی کشورها فقدان توان تکنیکی آنها بود.

☑ **عنوان: دسترسی غیر مجاز جلوه‌ای از جرائم رایانه‌ای نوین**

☑ **نویسنده: فرزاد تحیری** (دانشجوی کارشناسی ارشد رشته حقوق جزا و جرم شناسی دانشگاه مفید قم)

چکیده

دسترسی غیرمجاز از جمله جرائم رایانه‌ای صرف (محض) محسوب می‌شود. جرمی رایانه‌ای با ماهیت و مفهوم خاص می‌باشد که تا کنون به صورت اختصاصی بدان پرداخته نشده است؛ به همین دلیل، گاه در میان متخصصین (چه حقوقی و چه فنی) اصطلاحات و عباراتی دیگر به جای آن به کار می‌رود. عباراتی نظیر: «هکینگ»، «نفوذگری یا نفوذ یافتگی»، «دزدی رایانه‌ای»، «ورود غیر مجاز»، « دستیابی یا دستیافتگی» و... نشانه عدم مطالعه دقیق نسبت به جرم دسترسی غیر مجاز می‌باشد. در این مقاله سعی می‌نماییم ضمن ارائه مفهومی دقیق از دسترسی غیرمجاز و بیان وجوه اختلاف با سایر مفاهیم، به بررسی ماهیتی و ساختاری جرم دسترسی غیرمجاز نیز بپردازیم. همچنین، علاوه بر این، به مطالعه‌ای تطبیقی در سطح حقوق داخلی و بین‌الملل در خصوص دسترسی غیرمجاز خواهیم پرداخت.

کلید واژه ها

هکینگ – نفوذگری– دسترسی غیرمجاز– جرم رایانه‌ای صرف – امنیت سیستم و داده‌ها – حق محرمانگی

۱ – مقدمه

دسترسی غیر مجاز، به عنوان یکی از جرائم رایانه‌ای محض، از جمله جرائمی می‌باشد که دارای نقشی زاینده در ارتکاب سایر جرائم رایانه‌ای، خصوصاً جرائم رایانه‌ای محض می‌باشد. به همین دلیل در محیط سایبر[۱]، جرمی مادر تلقی می‌شود. ما در این مقدمه ابتدا، تاریخچه‌ای مختصر از این پدیده مجرمانه و مفاهیم اتخاذ شده توسط متخصصین را مورد اشاره قرار می‌دهیم و سپس به بیان ویژگی‌های دسترسی غیرمجاز و ارزش‌ها و منافع مورد تعرض در دسترسی غیرمجاز می‌پردازیم. آنگاه مختصراً، مطالعه‌ای آماری در خصوص دسترسی غیرمجاز را بیان می‌داریم و سرانجام، به ذکر جایگاه دسترسی غیرمجاز و نیزطبقه‌بندی‌های مختلف از آن می‌پردازیم.

۱-۱- پیدایش تاریخی دسترسی غیر مجاز در حقوق کیفری

بررسی پیرامون تاریخچه پیدایش و تحول جرم رایانه‌ای نیازمند رجوع به دهه «۱۹۶۰» میلادی است. در این دهه، اولین قضایای مربوط به جرائم رایانه‌ای ارتکاب یافت. در جامعه آمریکا، « قضیه رویس»[۲] موجب شد برای اولین بار، اذهان متوجه

سوء استفاده‌های رایانه‌ای شود. اولین گروه متجاوز موسوم به «باشگاه نمونه فنی راه آهن»[۳] در سال «۱۹۶۱» و مدتی کوتاه پس از اینکه دانشگاه« ام آی تی»[۴]، اولین رایانه «PDP»[۵] خود را دریافت کرد، در این دانشگاه تشکیل شد.[۶] در بررسی تاریخی دسترسی غیرمجاز، می‌بایست سابقه آن را از دستیابندگان غیرمجاز به سیستم‌های تلفنی آغاز نمود. به عبارت دیگر، بسیاری از اولین دستیابندگان غیرمجاز، فعالیت خود را به عنوان یک «فریکر»[۷] آغاز نمودند.

یکی از اولین« فریکرها»، «استوارت نلسون» بود. وی با تولید تون‌های دستیابی به خدمات راه دور شرکت تلفن، توانست از خدمات مجانی آن استفاده نماید. بعدها ساخت جعبه‌های آبی، قرمز و پنیر در همین راستا صورت گرفت. با اختراع اولین رایانه موسوم به «Altair 8800 » تجاوزگری نیز متولد گردید؛ زیرا، این وسیله این امکان را برای افراد به وجود آورد که برنامه‌نویسی را فرا گیرند. با اختراع «BBS »ها[۸] و توسعه آن، متجاوزان از آن برای ارتباط با یکدیگر و به اشتراک گذاردن منابع خویش استفاده نمودند. با ظهور شبکه‌ها، دسترسی غیرمجاز وارد مرحله جدیدی شد. در دهه «۱۹۹۰»، شبکه «آرپانت»[۹]، متوقف و اینترنت متولد گردید. با تولد اینترنت، موج وسیعی از دسترسی‌های غیرمجاز (نوین) آغاز شد:

دسترسی غیرمجاز به صندوق‌های پست‌الکترونیکی و بانک‌های اطلاعاتی مهم، دسترسی غیرمجاز به تارنماهای شرکت‌ها، مؤسسات و سازمان‌های دولتی و غیر دولتی مهم ایالات متحده، مانند: تارنماهای وزارت دادگستری، وزارت بازرگانی، سازمان اطلاعات مرکزی، سنا، نیروی هوایی، مجله نیویورک تایمز، شرکت مایکروسافت و غیره از این جمله‌اند.

در سال «۱۹۹۹» ، دو سوئدی به سیستم رایانه‌ای سازمان ملی فضا و هوای ایالات متحده و نیروهای مسلح این کشور دسترسی غیرمجاز یافتند. با ورود به سال «۲۰۰۰» ، یک تهاجم بزرگ وگسترده تارنماهای بزرگی چون «یاهو»[۱۰] و «آمازون»[۱۱] را، از کار انداخت.

۱-۲- مفاهیم، ویژگی‌ها، ارزش‌ها و منافع مورد تعرض در دسترسی غیرمجاز

در این قسمت به بیان مفاهیم دسترسی غیرمجاز و همچنین ارزش‌ها و منافع مورد تعرض که بی شک دلیل جرم‌انگاری آن محسوب می‌گردد، می‌پردازیم.

۱-۲-۱- مفاهیم دسترسی غیرمجاز

در میان متخصصین، (چه حقوقی و چه فنی) نسبت به مفهوم دسترسی غیرمجاز، وحدت نظر وجود ندارد. متخصصین فنی از عبارت «هکینگ»، استفاده می‌کنند و منظور از آن را «هر نوع حمله به سیستم‌های ایمن بیان می‌دارند.»[۱۲] برخی دیگر، «هکینگ» را در معنی محدودتر، «نفوذیابی» یا «نفوذگری»، ترجمه می‌کنند.[۱۳] و برخی دیگر، «هکینگ» را مترادف با دسترسی غیرمجاز می‌دانند.[۱۴] به نظر می‌رسد «هکینگ»، را نمی‌توان مترادف با دسترسی غیرمجاز تلقی نمود؛ زیرا «هکینگ»، چه در عنوان و چه در آماج و چه در نوع سیستم بر حسب ایمن یا غیر ایمن بودن و چه در وسعت شمول افعال مادی، با دسترسی غیرمجاز متفاوت است: اولا، «هکینگ»، عنوانی است اختصاصی که تنها در دانش فنی- مهندسی (علوم رایانه‌ای) به کار می‌رود و در این دانش، معنایی خاص و فنی دارد. ثانیاً، دسترسی غیرمجاز، راجع است به سیستم‌ها و داده‌های رایانه‌ای، در حالی که «هکینگ»، تنها راجع است به سیستم‌های رایانه‌ای. ثالثاً، دسترسی غیرمجاز راجع است به همه سیستم‌ها حتی «بدون محافظ»، در حالی که ایمن بودن سیستم‌ها از قیود تفکیک‌ناپذیر در «هکینگ» می‌باشد و رابعاً اینکه در دسترسی غیر مجاز صرف دسترسی به سیستم ها و داده‌های رایانه‌ای جرم می‌باشد در حالی که در «هکینگ»، علاوه بر دسترسی غیرمجاز اقداماتی دیگر نیز انجام می‌گیرد. این اقدامات عموماً ناظر است به تجزیه و تحلیل یا مداخله در عملکرد

پردازشی سیستم یا نسخه‌برداری از داده‌ها و یا ایجاد وقفه یا اختلال در سیستم و مانند آن، که هر کدام از این افعال، ممکن است دارای وصف مجرمانه باشد.

«نفوذگری» یا «نفوذیافتگی» را نیز نمی‌توان معادل یا ترجمه «هکینگ» دانست. زیرا همانطور که بیان نمودیم «هکینگ» تنها شامل صرف دسترسی غیرمجاز به سیستم‌های ایمن (نفوذ) نمی‌باشد. بلکه هرگونه تهاجم و حمله به سیستم‌های ایمن را در بر می‌گیرد. به همین دلیل در ترجمه هکینگ، به جای عبارت «نفوذگری»، پیشنهاد می‌نماییم از عبارت «تجاوز گری»،[۱۵] استفاده شود.

متخصصین حقوق کیفری رایانه نیز از عباراتی دیگر مانند نفوذ غیرمجاز، ورود غیرمجاز، دستیابی غیرمجاز استفاده می‌کنند که به زعم ما همه آنها در زیر مجموعه دسترسی غیرمجاز قرار می‌گیرند.

به این ترتیب، دسترسی غیر مجاز عبارت است از: « دسترسی بدون مجوز به سیستم‌ها یا داده‌های رایانه‌ای (جزئاً یا کلا) یا بدون نقض تدابیر ایمنی یا حفاظتی آنها»

۱-۲-۲- ویژگی‌های دسترسی غیرمجاز

دسترسی غیرمجاز، جرمی است که عموماً توسط افراد برنامه‌نویس و متخصص در علوم رایانه‌ای ارتکاب می‌یابد. جرمی با ماهیت کاملاً تکنیکی و فنی است و در میان جرائم رایانه‌ای از جمله جرائم رایانه‌ای محض تلقی می‌شود. در تقسیم‌بندی‌های سنتی از جرائم می‌توان آن را از زمره جرائم علیه اموال محسوب داشت. همچنین جرمی است عمدی، آنی، مطلق، غیر مشهود. عنصر مادی این جرم ناظر به افعال مثبت می‌باشد. از آنجایی که دسترسی غیرمجاز، در ارتکاب بسیاری از جرائم رایانه‌ای (خصوصاً جرائم رایانه‌ای محض) دارای تأثیر و نقش می‌باشد به عنوان جرمی مادر یا زاینده، معروف است.

۱-۲-۳- ارزش ها و منافع مورد تعرض در دسترسی غیرمجاز

دسترسی غیرمجاز، به مانند همه جرائم، ارزش‌ها و منافعی را مورد تعرض قرار می‌دهد. این تعرض در دسترسی غیرمجاز، متوجه امنیت و محرمانگی سیستم‌ها و داده‌های رایانه‌ای می‌باشد و به واقع دلیل جرم‌انگاری دسترسی غیرمجاز، نقض امنیت و محرمانگی سیستم‌ها وداده‌های رایانه‌ای است. منظور از امنیت سیستم‌ها، مصون بودن تمامیت و صحت داده‌ها و سیستم‌های رایانه‌ای از تعرض و منظور از محرمانگی سیستم‌ها و داده‌های رایانه‌ای، مصون بودن داده‌ها و سیستم‌های رایانه‌ای از هرگونه افشا، کسب اطلاع، رویت، مداخله، بررسی یا تجزیه و تحلیل در عملکرد یا فعالیت پردازشی می‌باشد.

۱-۳- آمار و حجم و وسعت خسارات در دسترسی غیر مجاز

در این قسمت ابتدا آمار دسترسی غیرمجاز و سپس حجم و وسعت خسارات وارده در اثر وقوع دسترسی غیرمجاز در سطح جهان و سپس در سطح ایران را مورد بررسی قرار می‌دهیم.

۱-۳-۱-در سطح جهان

در سطح جهان، رقم واقعی دسترسی‌های غیرمجاز و میزان خسارات وارده نامشخص می‌باشد. آمارها بر اساس گزارش‌های رسمی یا دستگیری‌های انجام شده استوار می‌باشد و الا بسیاری از دسترسی‌های غیرمجاز یا کشف نمی‌شوند و یا اینکه غیر قابل تعقیب می‌باشند.

۱-۳-۱-۱-آمار

در خصوص آمار جرائم رایانه‌ای در سطح جهان هنوز آماری که جامع و دقیق باشد ارائه نشده است «علت نامشخص بودن آمار واقعی جرایم رایانه‌ای فقدان تعریف واضح و مشخص، عدم توانایی بزه‌دیدگان در تشخیص بزه‌دیدگی، فقدان سیستم‌های آماری در سیستم‌های قضایی و پلیسی برای کلاسه‌بندی جرایم رایانه‌ای و دلایل متعدد دیگر می‌باشد. با این وجود، منابع متعدد آمارهای مختلفی را گزارش می‌کنند.»[۱۶] «بررسی آمار جرائم رایانه‌ای جهان بیانگر این واقعیت است که طی سال‌های ۱۹۹۶ الی ۱۹۹۹ برخی از کشورها شاهد ۱۶۰۰ درصد رشد در اینگونه جرائم بوده‌اند که شامل نفوذ غیرقانونی، رمز شکنی، چاپ تصاویر یا تبلیغات مبتذل، خسارت به دیگران، تقلب در خریدهای اینترنتی، تعرض به حقوق مالکیت معنوی و دیگر موارد می‌شده است.

بر پایه گزارش مرکز هماهنگی گروه واکنش سریع در موارد اضطراری رایانه‌ای،[۱۷] شمار رویدادهای گزارش شده درباره نقض حریم امن رایانه‌ها، در ۹ ماهه اول سال ۲۰۰۰ نسبت به شمار کل رویدادهای گزارش شده در سال ۱۹۹۹ پنجاه و چهار درصد افزایش نشان می‌دهد. افزون بر این، موارد بی‌شماری از دسترسی‌های غیرمجاز و تخریب در سراسر جهان هنوز از دید گزارش‌ها پنهان مانده‌اند. دلیل این امر این است که بزه‌دیدگان این جرائم، از آشکار شدن نقاط آسیب‌پذیر خود و احتمال ارتکاب جرائم مشابه و از دست رفتن اعتماد عمومی هراس دارند.»[۱۸]

در ادامه وضعیت آماری دسترسی غیرمجاز را در میان سایر جرائم رایانه‌ای در برخی از کشورها نشان می‌دهیم:

۱-۳-۱-۱-۱- سوییس

در سوییس، در بین سال‌های «۱۹۹۵ تا ۱۹۹۹» میزان محکومیت‌های صادر شده در خصوص ورود غیرمجاز به یک سیستم پردازنده داده‌ها، بسیار اندک می‌باشد: در سال «۱۹۹۵» هیچ مورد محکومیت، در سال «۱۹۹۶» یک مورد، در سال«۱۹۹۷» هیچ مورد و در سال‌های «۱۹۹۸» و «۱۹۹۹» هر سال یک مورد حکم محکومیت وجود داشته است.[۱۹]

۱-۳-۱-۱-۲- استرالیا

در استرالیا، نشانه‌ها حاکی از این است که جرائم اینترنتی در حال افزایش می‌باشد. به عنوان مثال، «گروه واکنش سریع در موارد اضطراری رایانه‌ای استرالیا» (AusCERT)، که سازمانی جهت مساعدت در جلوگیری ازحملات رایانه‌ای می‌باشد، تأیید نموده است که استرالیا شاهد افزایش قابل توجهی در شمار جرائم اینترنتی در سال‌های اخیر بوده است.

در سال ۲۰۰۰، مجموعاً ۱۹۷/۸ حادثه امنیتی رایانه‌ای به AusCERT گزارش شدکه این رقم نسبت به میزان گزارش‌های سال «۱۹۹۹» ، چهار برابر افزایش داشت.

در یک پژوهش غیر رسمی توسط وکلای قانونی پلیس استرالیا در امور رایانه‌ای، در سپتامبر ۲۰۰۱، جرائم زیر شناسایی شد:

کلاهبرداری (کارت اعتباری و پست الکترونیکی)، نفوذ به سیستم‌های رایانه‌ای و ایجاد آشفتگی، هرزه‌نگاری از کودکان، هویت تقلب، اقدام جهت دسترسی به اطلاعات محرمانه، موارد مربوط به مواد مخدر، تقلب در بازار سهام، جمع‌آوری غیر قانونی اعانه.

۱-۳-۱-۱-۳- چین

در چین، افزایشی قابل توجه در میزان جرائم رایانه‌ای گزارش شده است. طبق آمار ارائه شده توسط پلیس، شواهد حاصله نشانگر افزایش معادل دو برابر در هر سال می‌باشد. این جرائم رایانه‌ای عموماً مربوط به هرزه‌نگاری، ویروس‌ها، دسترسی غیرمجاز و دیگر جرائم رایانه‌ای می‌باشد. آمار ارائه شده توسط چین در چهار سال اخیر، افزایشی هشدار دهنده را در وقوع چنین حوادثی نشان می‌دهد. پلیس چین در سپتامبر ۲۰۰۱ جرائم زیر را به عنوان بیشترین جرائم رایانه‌ای در چین، شناسایی کرد:

هرزه‌نگاری، انتشار اخبار جعلی و کلاهبرداری، دسترسی غیرمجاز، تقلب کارت اعتباری، نفوذ به سیستم رایانه‌ای و ایجاد آشفتگی، ویروس‌ها

۱-۳-۱-۱-٤- هنگ کنگ

پس از چند سال افزایش قابل توجه در میزان جرایم رایانه‌ای ازسال ۱۹۹۸، به نظر می‌رسد که هنگ‌کنگ تا سال ۲۰۰۱ کاهشی را در میزان جرائم گزارش شده، تجربه می‌کند (جدول ۱). این کاهش را می‌توان در انواع دسترسی‌های غیرمجاز به رایانه، که درمجموع بالاترین میزان جرایم رایانه‌ای را تشکیل می‌دهد، مشاهده کرد.

عنوان جرم	۱۹۹۸	۱۹۹۹	۲۰۰۰	۲۰۰۱
دسترسی غیرمجاز به رایانه از طریق ارتباطات راه‌دور	۱۳	۲۳۸	۲۷۵	۳۳
دسترسی به رایانه با نیت بزه‌کاری یا تقلب				۱۸
صدمات کیفری	۳	۴	۱۵	۲۷
کسب مالکیت بوسیله جعل	۱	۱۸	۲۹	۳۲
کسب خدمات بوسیله جعل				۱۳
سرقت‌های متفرقه	۰	۰	۰	۱۶
موارد دیگر *	۱۷	۵۷	۴۹	۱۳
جمع	۳۴	۳۱۷	۳۶۸	۲۳۵

جدول ۱

* موارد دیگر مربوط جرائم شامل: تهدیدات بمب‌گذاری، ایجاد کیفری، اخاذی، قمار و جعل اسکناس، انتشار فحشاء، جرائم جنسی، و غیره می‌شود.

۱-۳-۱-۱-۵- هـــــند

در هند، جرائم اینترنتی متعددی در رابطه با مواردی چون «هکینگ»، دزدی از زمان اینترنت، تولید یا انتشار ویروس‌ها، خدشه‌دارکردن عفت زنان با استفاده از شبکه جهانی، نقض حق‌طبع و نشر، تارنماهای هرزه‌نگاری، تقلب کارت‌های اعتباری گزارش می‌شود. در همین اواخر، چند تارنمای دولتی مورد نفوذ و آشفتگی قرار گرفته‌اند. همچنین جرائم مرسومی گزارش شده‌اند که در آنها از رایانه استفاده شده است.

۱-۳-۱-۱-۶- ژاپـــن

در این کشور دسترسی غیرمجاز در میان سایر جرائم رایانه‌ای در سال ۲۰۰۰، ۳۱ مورد و در سال ۲۰۰۱، ۳۵ مورد گزارش شده است «جدول ۲» وضعیت دسترسی غیرمجاز را در میان سایر جرائم رایانه‌ای در سال‌های ۱۹۹۸ تا ۲۰۰۱ نشان می‌دهد:

طبقه‌بندی جرائم	۱۹۹۸	۱۹۹۹	۲۰۰۰	۲۰۰۱
جرائم علیه رایانه / ثبت الکترومغناطیسی	۲۹۹	۱۱۰	۴۴	۶۳
کلاهبرداری رایانه‌ای	۲۸۷	۹۸	۳۳	۴۸
تخریب رایانه	۸	۷	۲	۴
ثبت الکترومغناطیسی اسناد	۴	۵	۹	۱۱
جرائم با بکارگیری شبکه‌های رایانه‌ای	۱۱۶	۲۴۷	۴۸۴	۷۱۲
انشار ادبیات قبیح	۸۰	۱۴۷	۱۵۴	۱۰۳
جرائم مربوط به هرزه‌نگاری از کودکان	ـــ	۹	۱۲۱	۲۴۵
تقلب	۱۱	۲۳	۵۳	۱۰۳
هتک حرمت	۲	۱۲	۳۰	۴۲
جرائم بر علیه حق طبع و نشر	۱۷	۲۱	۲۹	۲۸
موارد دیگر	۶	۳۵	۳۱	۳۵
دسترسی غیرمجاز	ـــ	ـــ	۳۱	۳۵
جمع	۴۱۵	۳۵۷	۵۵۹	۸۱۰

جدول ۲

۱-۳-۱-۱-۷- کره

در کره نفوذ به سیستم‌های رایانه‌ای در بین سال‌های ۱۹۹۷ تا ۲۰۰۱ افزایش قابل توجهی داشته «جدول ۳» این افزایش را در میان سایر جرائم ارتکاب شده (که منتهی به دستگیری گشته) نشان می‌دهد:

	۱۹۹۷	۱۹۹۸	۱۹۹۹	۲۰۰۰	۲۰۰۱ ماه‌های ۱تا۱۰
جرائم عمده اینترنتی	۶	۲۱	۲۶	۳۶۳	۵/۶۷۳
نفوذ به سیستم رایانه‌ای و ایجاد آشفتگی	۶	۱۶	۲۳	۳۶۰	۵/۶۰۴
ویروس	۰	۵	۳	۳	۶۹
جرائم دیگر اینترنتی	۱۳۵	۴۴۵	۳/۰۶۳	۱/۸۲۷	۱۱/۵۲۸
جمع	۱۴۱	۴۶۶	۲/۰۸۹	۲/۱۹۰	۱۷/۲۰۱

جدول۳

۱-۳-۱-۱-۸- نـــپال

در این کشور، جرائم اینترنتی متعددی مثل دزدیدن از زمان اینترنت، دسترسی غیرمجاز به سیستم‌های ایمن رایانه‌ای، نفوذ و ایجاد آشفتگی در سیستم امنیتی، پخش ویروس‌ها، تارنماهای هرزه‌نگاری، تقلب کارت‌های اعتباری و نقض حق طبع و نشر، وجود دارد. در نپال این جرائم رسماً گزارش نمی‌شوند. یک جرم اینترنتی به تازگی در مورد نفوذ و ایجاد آشفتگی گزارش شده است: تمامی تارنماهای وب دولتی مورد هجوم و آشفتگی قرار گرفتند. نفوذگران سعی به نفوذ و آشفته‌سازی ارائه کننده خدمات اینترنتی [۲۰] که خدمات‌دهنده اکثر تارنماهای وب دولتی بود، نمودند. در حال حاضر، ۱۵ سرویس‌دهنده اینترنت و ۰/۵ میلیون کاربر شبکه جهانی تا سال ۲۰۰۱ وجود دارند.[۲۱]

۱-۳-۱-۲- حجم و وسعت خسارات وارده

در شهریور ماه سال ۱۳۷۸ یک مهاجم اینترنتی در گوشه نامعلومی از جهان هنگامی که احزاب سیاسی استرالیا، سرگرم مبارزات انتخاباتی بودند، وارد تارنمای وب حزب حاکم لیبرال استرالیا شد و ضمن ایجاد تغییرات در محتوا، مطالب آن را به صورت مضحکی در آورد و در پایان چند عکس مستهجن نیز ضمیمه آن کرد. این عمل مهاجم ناشناس، لطمه شدیدی به حیثیت حزب لیبرال وارد ساخته بود. [۲۲] همچنین در مورد دیگری، مهاجم یا مهاجمان ناشناس با ورود به سیستم رایانه‌ای دانشگاه استانفورد آمریکا، رمز پست الکترونیکی ۴۵۰۰ نفر از دانشجویان و استادان را مورد دستبرد قرار دادند. مهاجمان برای سه هفته بدون اینکه کسی متوجه شود به مطالب پست‌های الکترونیکی این دانشگاه دسترسی داشته‌اند.[۲۳]

نفوذ به تارنماهای خبری یکی دیگر از مواردی است که جداً، مشکل آفرین شده است. مسأله وقتی نگران‌کننده و مشکل آفرین خواهد بود که اخبار از سوی افراد متخصص و سازمان‌های ویژه و به صورت کاملاً حرفه‌ای و به شکل تغییرات کاملاً جزیی، ولی تعیین‌کننده، دستکاری شود و به نحوی این عمل انجام گیرد که تشخیص تغییر انجام شده غیرممکن باشد به عنوان مثال تارنمای« USA Today»که یکی از تارنماهای خبری در اینترنت می‌باشد و ماهانه حدود ۹ میلیون بازدید کننده دارد، بارها مورد حمله متجاوزان قرار گرفته است. همچنین است تارنمای خبری«نیویورک تایمز» و «یاهو» که بارها مورد حمله هکرها قرار گرفته‌اند.[۲۴]

«کانون وکلای آمریکا در سال ۱۹۸۷ دست به انجام مطالعاتی زد: از ۳۰۰ شرکت و اداره دولتی ۷۲ واحد ادعا داشتند که در فاصله زمانی ۱۲ ماه قبل از شروع مطالعات مذکور بزه‌دیده جرائم رایانه‌ای بوده‌اند و طبق برآورد، خساراتی بین ۱۴۵ تا ۷۳۰ میلیون دلار را متحمل شده‌اند. آمار جمهوری فدرال آلمان بیانگر ۳۰۶۷ مورد است که در طول سال ۱۹۸۷ به وسیله پلیس بررسی شده است. ۲۷۷۷ مورد از قضایا را پلیس کلاهبرداری رایانه‌ای، موضوع ماده ۲۶۳ الف مجموعه قوانین جزایی آلمان، تلقی کرده است و این موارد بیشتر از طریق ماشین‌های پرداخت کننده اتوماتیک انجام شده است. ۱۵۰مورد، حکم محکومیت ۱۶۹ قضیه، ناظر به جعل داده‌ها، ۷۲ مورد تغییر داده‌ها و سابوتاژ و ۴۹ مورد جاسوسی داده‌ها گزارش شده است. ۷۱ درصد مظنونین بالای ۲۱ سال سن داشتند از طرفی خسارات وارده نیز ارقام زیادی را نشان می‌دهد. در آلمان سوء استفاده‌های رایانه‌ای بین ۲ تا ۳ میلیون مارک در طی ده سال گذشته خسارت وارد کرده است. برآورد آمریکا بیانگر سالانه ۱۰۰ تا ۳۰۰ میلیون دلار خسارات وارده از جرائم رایانه‌ای است که البته این رقم طبق برآورد «OECD»کمتر از مبلغ واقعی آن است.»[۲۵]

بر اساس گزارش مندرج در مجله شبکه و ارتباطات در سال ۱۹۹۵ حدود ۳۷۵/۳ میلیون دلار به صنعت ارتباطات، در سراسر جهان خسارت وارد شده و این رقم فقط در اثر نفوذ به شبکه‌های ارتباطی تلفنی پدید آمده است. بر اساس این مقاله که

در یکی از روزنامه‌های سانفرانسیسکو درج شده بود ارتکاب اعمال غیر قانونی در فضای مجازی در انگلستان رو به افزایش نهاده است.

بر اساس یک نظر سنجی که از ۲۴۶ شرکت به عمل آمده در فاصله میان سال‌های ۱۹۸۵ تا ۱۹۹۳ سرقت اطلاعات انحصاری از طریق سیستم‌های رایانه‌ای ۲۶۰ درصد افزایش یافته است.

در سال ۱۹۹۱ عقیده بر این بود که حجم خسارت ناشی از کلاهبرداری رایانه‌ای ۵ بیلیون دلار است همچنین بر اساس گزارشات تنظیمی در همان سال حجم خسارات ناشی از جرایم رایانه‌ای در انگلستان، سالانه ۲/۵ میلیون پوند بوده است.

یکی از دلایل فقدان آمارهای واقعی از جرایم رایانه‌ای عدم توانایی بزه‌دیدگان در تشخیص بزه‌دیدگی و یا عدم تمایل آنها به گزارش موضوع به پلیس می‌باشد. برای مثال رشد اینترنت باعث افزایش میزان خسارات ناشی از جرایم رایانه‌ای شده و تخمین زده می‌شود که این میزان در آمریکا ۱۰ بیلیون دلار و در انگلستان فقط خسارات حاصله از کلاهبرداری رایانه‌ای ۵ بیلیون پوند در سال است.

تهدیدات علیه امنیت اطلاعات در زمره یکی از ۱۰ تهدید مهم که متوجه شرکت‌های آمریکایی است، قرار دارد.

این تهدید در ردیف چهارم جای دارد. سرقت اطلاعات یک تهدید اصلی است و هر ساله بیلیونها دلار خسارت به بار می‌آورد. کمپانی‌های آمریکایی همواره نگران این موضوع می‌باشند.[۲۶]

۱-۳-۲- در سطح ایران

در ابتدا آمار و سپس میزان خسارات وارده در اثر وقوع دسترسی غیرمجاز را در ایران بررسی می‌کنیم

۱-۳-۲-۱- آمار

تا کنون از جانب هیچ مرجع رسمی آماری در خصوص میزان دسترسی‌های غیرمجاز منتشر نشده است و تنها تا به حال چندین مورد انگشت شمار در اخبار منتشر شده است که در قسمت بعد بیان می‌نماییم. به نظر می‌رسد رقم سیاه در این خصوص در ایران بالا باشد؛ زیرا، اولاً سیستم‌ها و شبکه‌های رایانه‌ای به طور مناسب ایمن نشده‌اند و اصولا به دلیل امکانات کم مادی چنین هزینه‌های وجود ندارد. ثانیاً، بسیاری از مدیران سیستم‌ها فاقد اطلاعات تخصصی و حتی عمومی می‌باشند و گاه از روی بی‌احتیاطی زمینه دسترسی غیرمجاز را فراهم می‌کنند. ثالثاً، تا به حال دسترسی غیرمجاز به مانند سایر جرائم رایانه‌ای جرم‌انگاری نشده است. نویسنده بنا به یک تحقیق و نظر سنجی غیر رسمی و محرمانه از ۴۰۰ پرسش شونده (۷۰ شرکت خصوصی رایانه‌ای- اینترنتی و ۳۴۰ کاربر اینترنتی و غیر اینترنتی در کلیه سطوح حرفه‌ای، متوسط و آماتور) به این نتیجه رسیده است میزان دسترسی غیرمجاز در ایران بالاو در حال افزایش می‌باشد و بنا بر تحقیقی محرمانه دیگر از ۱۳۰ هکر (در تمای اقسام آنها) به این نتیجه رسیده است که غالباً دلایل هکرها برای دسترسی غیرمجاز به ترتیب دلایل احساسی- روانی، مالی، علمی – آموزشی و سیاسی می‌باشد.

۱-۳-۲-۲- حجم و وسعت خسارات وارده

در تابستان «۱۳۸۱» فردی که خود را « اسپایدر من»[۲۷] می‌نامید، با استفاده از ضعف امنیتی برخی سیستم‌های خدمات‌دهنده [۲۸] وارد سیستم شده و با به دست گرفتن کنترل خدمات دهنده‌های میزبان[۲۹] موفق گردید، بیش از ۱۸۰ تارنمای فارسی و ایرانی را مورد تخریب قرار دهد. وی در بعضی از سیستم‌های میزبان، تمامی پوشه‌های موجود در سیستم را، حذف نمود و خسارات زیادی به صاحبان آنها و نیز دارندگان تارنماها، وارد ساخت. وی طی ارسال نامه الکترونیکی به برخی

مدیران تارنماها، دلیل این اقدام را نشان دادن ضعف امنیتی خدمات دهنده‌های ایرانی معرفی نمود. وی مجدداً در پاییز همان سال، با ورود به سیستم خدمات‌دهنده میزبان، صفحه نخست بیش از دویست تارنما را عوض نموده و به جای آن تعدادی زیادی صفر و یک قرارداد.

در اواخرسال ۱۳۸۱، گروهی که خود را« اسپایدر وب» می‌نامیدند، با نفوذ به سیستم میزبان، تعدادی از تارنماهای فارسی را تخریب نمودند. این گروه، اقدام به تغییرات در صفحه نخست برخی تارنماها نمودند. این گروه در برخی تارنماها تصویری از تارهای عنکوت قرارداده بودند.

در اواخر سال ۱۳۸۱، گروهی که خود را«مش قاسم» معرفی می‌کرد توانست با ورود به سیستم خدمات‌دهنده میزبان « فراهاست »که تارنماهای زیادی را میزبانی می‌نماید، دسترسی به بیش از یکصد تارنمای ایرانی را قطع نماید و خساراتی را وارد سازد. این گروه تا اوایل سال ۸۲ به نفوذ خود به خدمات دهنده‌ها ادامه داده و از جمله به خدمات‌دهنده میزبان «بلاگ اسکای» که یک خدمات‌دهنده فارسی «بلاگ‌نویسی»[۳۰] می‌باشد نفوذ نمودند.

در تابستان ۱۳۸۲ فردی که خود را«مرد محافظ»[۳۱] می‌نامید، توانست با همکاری عده‌ای دیگر با دست آوردن کلمه عبور «پنل دامین» یک شرکت ثبت نام حوزه[۳۲] و ارائه دهنده خدمات اجاره فضای اینترنتی ایرانی و ورود به سیستم آن مشخصات نام‌های حوزه را تغییر داده وبا تغییر «DNS »، [۳۳] برخی تارنماها را (نام‌های حوزه) به سمت تارنمایی مجانی (خدمات دهنده میزبان)، هدایت نماید. این فرد پس از انجام تغییرات کلمه عبور دسترسی به «پنل دامین»، دارندگان آن را از دسترسی محروم نمود و در عین حال با متوقف شدن فعالیت تارنماهای ثبت شده، خسارات زیادی را به دارندگان تارنماها که از جمله تارنماهای مهمی بوده‌اند وارد ساخت. این گروه در مدتی اندک شناسایی و دستگیر شدند. این نخستین مورد پی‌گیری شده و به نتیجه رسیده می‌باشد.

در پاییز ۱۳۸۲، ماموران توانستند فردی را که توانسته بود از طریق اینترنت به سیستم شرکتی که مرکز انفورماتیک بانک‌های کشور بوده نفوذ نماید و به مرکز کل اطلاعات بانک (ملی) دسترسی پیدا کند را شناسایی و دستگیر نمایند او با استفاده از یک حساب بانکی جعلی، ارقام ریالی را به تدریج از سیستم‌های خود پرداز به حساب خود واریز می‌نمود. وی توانست در حدود ۶۰ میلیون تومان وجه را به حساب خود واریز نماید. وی نهایتاً توسط پلیس پس از چندین ساعت عملیات تعقیب و مراقبت دستگیر شد.[۳۴]

آنچه از مطالب فوق بر می‌آید این است که چنانکه ملاحظه می‌گردد، در سال‌های اخیر در ایران، با افزایش استفاده از خدمات شبکه‌های مختلف رایانه‌ای، خصوصاً شبکه جهانی اینترنت، بر تعداد متجاوزان رایانه‌ای نیز افزوده شده که این امر خود مسائل و مشکلاتی را برای اشخاص، خصوصاً شرکت‌های خصوصی خدمات دهنده، ایجاد نموده است؛ مشکلی که هر روزه موجب افزایش میزان خسارت‌های مختلف می‌گردد.

۱-٤- جایگاه و طبقه بندی دسترسی غیر مجاز

دسترسی غیرمجاز، از بعد حقوق جزای سنتی و حقوق جزای رایانه‌ای دارای جایگاهی می‌باشد. همچنین می‌توان برای آن تقسیم بندی‌هایی ذکر نمود.

۱-٤-۱- جایگاه دسترسی غیرمجاز

برخی دسترسی غیرمجاز را، در زیر مجموعه جرائم علیه تکنولوژی محض قرارداده‌اند.[۳۵] برخی دیگرآن را از زمره جرائم علیه محرمانگی و تمامیت و در دسترس بودن سیستم‌ها و داده‌های رایانه‌ای دانسته‌اند.[۳۶] دسترسی غیرمجاز را از نظر حقوق جزای رایانه‌ای می‌توان از زمره جرائم رایانه‌ای محض دانست؛ زیرا اولاً، از جرائم مرتبط با سیستم‌های رایانه‌ای است و ثانیاً، تنها در محیط سیستم‌های رایانه‌ای و سایبر، قابل ارتکاب می‌باشد از نظر حقوق جزای سنتی دسترسی غیرمجاز از زمره جرائم علیه اموال تلقی می‌شود. برخی نیز آن را از زمره جرائم مالی یا اقتصادی دانسته‌اند [۳۷]

۱-٤-۲- طبقه بندی دسترسی غیر مجاز

دسترسی غیرمجاز بر اساس آماج، (شامل: دسترسی به سیستم‌ها و دسترسی به داده‌های رایانه‌ای)، محیط وقوع جرم، (محل فیزیکی سیستم‌ها، دسترسی در داخل یا خارج از شبکه، دسترسی بر اساس دوری و نزدیک سیستم‌ها نسبت به مرتکب شامل دسترسی از راه نزدیک و دسترسی از راه دور)، تمهیدات حمایتی و حفاظتی، (سیستم‌های محافظت شده و بدون محافظ، سیستم‌های حمایت شده و بدون حمایت، دسترسی با نقض و بدون نقض تدابیر حفاظتی)، نتیجه ارتکاب (مطلق و مقید)، شیوه ارتکاب، (دسترسی ساده یا محض، کسب اطلاع به نحو غیر مجاز، تحصیل اطلاعات به نحو غیر مجاز) قابل تقسیم می‌باشد.

۲- دسترسی غیرمجاز در حقوق کیفری

در این قسمت به مطالعه ساختاری دسترسی غیر مجاز شامل ارکان تشکیل‌دهنده آن و مقایسه آن با سایر جرائم رایانه‌ای و نیز طرفین جرم شامل مرتکبین و بزه‌دیدگان دسترسی غیرمجاز می‌پردازیم.

۲-۱- ساختار دسترسی غیرمجاز

منظور از ساختار دسترسی غیرمجاز عبارت است از مجموعه ارکان تشکیل‌دهنده جرم و مقایسه ماهیتی آن با سایر جرائم رایانه‌ای.

۲-۱-۱- ارکان تشکیل‌دهنده

در این قسمت، ارکان تشکیل‌دهنده جرم دسترسی غیرمجاز (شامل رکن مادی و معنوی) را بیان می‌داریم و رکن قانونی آن را به هنگامی که به بیان پاسخ‌های کیفری می‌پردازیم بیان خواهیم داشت.

۲-۱-۱-۱- رکن مادی

در این جا ابتدا، شیوه‌های ارتکاب دسترسی غیرمجاز و سپس مراحل ارتکاب را، بیان می‌داریم.

۲-۱-۱-۱-۱- شیوه ها و طرق دسترسی غیر مجاز

شیوه‌های دسترسی غیرمجاز را می‌توان به شیوه‌های فنی، (برخی از این شیوه‌ها عبارتند از دسترسی به کلمات عبور[۳۸]، دسترسی از طریق درهای پشتی[۳۹]، دسترسی از طریق اسب‌های تروا[۴۰]، دسترسی از طریق مودم، دسترسی به داده‌های رمزگذاری شده یا مخفی) و شیوه‌های غیر فنی (شامل شیوه‌های مبتنی بر دانش مهندسی اجتماعی[۴۱]، آشغال گردی[۴۲]، برقراری ارتباط دوستانه با مدیر سیستم[۴۳]، جعل عنوان، نشان دادن خود به جای کاربر مجاز و...) تقسیم نمود.

۲-۱-۱-۱-۲- مراحل فرآیند ارتکاب دسترسی غیرمجاز

مراحل ارتکاب را می‌توان به عنوان یک فرآیند از لحظه شروع تا پایان از نظر فنی و حقوقی تقسیم نمود. از نظر فنی شامل مراحل: انتخاب هدف، جمع‌آوری اطلاعات و سازمان‌دهی آنها، طرح ریزی حمله، اجرای حمله و پاکسازی حمله می‌باشد و از نظر حقوقی شامل مراحل: قصد ارتکاب، اجرای عملیات مقدماتی، شروع به جرم و اجرای آن می‌باشد. شایان ذکر است که

مراحل جمع‌آوری اطلاعات و سازماندهی آنها و طرح‌ریزی حمله از بعد حقوقی بـه عنـوان عملیـات مقـدماتی جـرم محسـوب می‌شوند همچنین بر خلاف نظر عده‌ای که معتقدند دسترسی غیرمجاز شروع به جرم ندارد نویسنده معتقد اسـت دسترسـی غیرمجاز دارای شروع به جرم می‌باشد شناخت وتشخیص شروع به جرم در دسترسی غیرمجاز به میزان قابل توجهی به شیوه‌ها و طرق مختلف دسترسی غیرمجاز بستگی دارد به همین دلیل امری کاملا تخصصی و فنی می‌باشد.

۲-۱-۱-۲- رکن معنوی

دسترسی غیرمجاز از زمره جرائم عمدی تلقی می‌شود. انگیزه در دسترسی غیرمجاز، بدون اینکه تـاثیری در ماهیـت جـرم داشته باشد، مختلف و متنوع می‌باشد.

۲-۱-۱-۲-۱- قصد مجرمانه

با توجه به اینکه دسترسی غیرمجاز جرمی مطلق محسوب می‌شود و مقید به هیچ نتیجه‌ای نمی‌باشد هیچ قصـد خـاص و ویژه‌ای نیاز ندارد به همین دلیل برای تحقق عنصر معنوی تنها سوء نیت عام کفایت می‌کند مرتکب می‌بایسـت عامـداً و عالمـاً مرتکب دسترسی غیرمجاز شود.

۲-۱-۱-۲-۲- انگیزه مجرمانه

این انگیزه‌ها را می‌توان شامل انگیزه‌های شرافتمندانه شامل: بالا بردن امنیت سیستم‌ها، مراقبـت از سیسـتم‌هـا در برابـر آسیب، کمک به پیشرفت دانش فنی و مهندسی و... و غیر شرافتمندانه شـامل: غـرض ورزی و انتقـام جـویی، کسـب شـهرت، انگیزه‌های مالی، حسادت و.. دانست شایان ذکر است که انگیزه‌های یاد شده هیچ تـأثیری در ماهیـت جـرم نـدارد و در نهایـت ممکن است به عنوان عاملی تخفیف دهنده محسوب شود.

۲-۱-۲- دسترسی غیر مجاز و جرائم رایانه ای دیگر

دسترسی غیرمجاز، «عاملی محرک» در ارتکاب سایر جرائم رایانه‌ای (خصوصاً جرائم رایانه‌ای محض) مـی باشـد. غالـب دستیابندگان غیرمجاز پس از دسترسی به سیستم به صرف دسترسی بسنده نکرده و اقـداماتی دیگـر کـه ممکـن اسـت دارای وصف مجرمانه نیز باشد انجام می‌دهند. نسخه‌برداری از داده‌ها، اختلال در سیستم انتشار برنامه‌های مخـرب و... از ایـن جملـه می‌باشد. دسترسی غیرمجاز علاوه بر اینکه «جرمی محرک»[۴۴] می‌باشد، «جرمی مادر»[۴۵] نیز تلقی مـی‌شـود زیـرا جرمـی است که جرائمی دیگر را به دنبال دارد. به عبارت دیگر زاینده جرائم دیگر هم می‌باشد (این جـرائم عمومـاً از جـرائم رایانـه‌ای محض می‌باشد) از منظر جرم شناسی،کنترل و بازدارندگی دسترسی غیرمجاز در کنترل و کاهش میزان وقـوع جـرائم رایانـه‌ای خصوصاً جرائم رایانه‌ای محض مؤثر می‌باشد. دسترسی غیرمجاز در برخی از جرائم رایانه‌ای محض به عنـوان مقدمـه ارتکـاب محسوب می‌شوند. این جرائم که شبیه دسترسی غیرمجاز می‌باشند عبارتند از: شنود غیر مجاز[۴۶]، جاسوسی رایانه‌ای، سـرقت رایانه‌ای. در برخی دیگر از جرائم رایانه‌ای و شاید غالب آنها، دسترسی غیرمجاز، تسهیل کننده وقوع می‌باشند و در برخی مـوارد دیگر، دسترسی غیرمجاز هیچ نقشی در ارتکاب ندارد .این جرائم عموماً جرائمی می‌باشند که در آن سیسـتم‌هـای رایانـه‌ای بـه عنوان ابزار و وسیله ارتکاب جرم مورد استفاده قرار می‌گیرند.

۲-۲- مرتکب و بزه‌دیده دسترسی غیرمجاز

در این قسمت ابتدا، به بررسی مرتکبین دسترسی غیرمجاز و نیز انواع آنها از بعد فنی و حقوقی و سپس دلایل بزه‌کاری، آنگاه، به بررسی بزه‌دیدگان دسترسی غیرمجاز می‌پردازیم. در قسمت اخیر انواع بزه‌دیدگان، دلایل بزه‌دیدگی، آثار بزه بر بزه‌دیدگان و سرانجام طرق حمایت از بزه‌دیدگان را مورد اشاره قرارخواهیم داد.

۲-۲-۱- مرتکب

دسترسی غیرمجاز، از جمله جرائمی می‌باشد که به دانش فنی و مهندسی ویژه نیازمند می‌باشد. اکثر دستیابندگان غیرمجاز از افراد برنامه‌نویس ماهر می‌باشند که هم تحصیلات بالایی در رشته مربوطه دارند و هم اینکه هزینه‌های زیادی را برای یادگیری برنامه‌نویسی نموده‌اند. این افراد عموماً از نظر امکانات مادی (اعم از وسایل و تجهیزات سخت‌افزاری و نرم‌افزاری و نیز وضعیت مالی) در سطح بالایی می‌باشند. عموماً افرادی منظم و از نظر اجتماعی سازش یافته و انطباق پذیرند. افرادی می‌باشند که قواعد حاکم بر فعالیت‌های حرفه‌ای خود را کراراً نقض می‌نمایند. به همین دلیل می‌توان اکثر دستیابندگان غیرمجاز (حرفه‌ای) را از جمله مجرمین یقه سفید دانست.[۴۷] در واقع برخی از مجرمین یقه سفید را می‌توان دستیابندگان غیرمجاز حرفه‌ای به سیستم‌های رایانه‌ای دانست.[۴۸]

۲-۲-۱-۱- انواع مرتکبین

مرتکبین را می‌توان از نظر حقوقی و فنی دسته بندی نمود: از نظر فنی، همانطور که بیان نمودیم، به «هکر»، موسوم می‌باشند. «هکرها»، از نظر فنی بر حسب میزان فعالیت، (شامل هکرهای اهل آزمایش و تجربه[۴۹]، هکرهای خرابکار[۵۰]، هکتیویستها[۵۱]، تبهکاران سایبر[۵۲]، هکرهای جنگجو[۵۳])، بر حسب هدف، (شامل: هکرها و فریکرها)، بر حسب شیوه رفتار، (شامل: هکرهای کلاه سفید[۵۴]، کلاه خاکستری[۵۵]، کلاه صورتی[۵۶]، کلاه سیاه [۵۷]) بر حسب سطح مهارت، (شامل: کاربران برنامه‌های بچه‌گانه[۵۸]، پویش گران سیستم‌های رایانه‌ای [۵۹] ، برنامه نویسان یا هکرهای واقعی[۶۰] قابل دسته‌بندی می‌باشند از نظر حقوقی نیز دستیابندگان را می‌توان بر حسب توصیف مجرمانه شامل: فاعلین جرم (مباشرین و شرکا در جرم) و معاونین جرم، بر حسب آماج به نفوذگر یا نفوذ یابنده (فردی که به سیستم‌های ایمن عمداً و بدون مجوز با نقض تدابیر ایمنی و حفاظتی آنها دسترسی پیدا می‌کند) و دستیابنده صرف (فردی که به سیستم‌ها و داده‌های رایانه‌ای عمداً و بدون مجوز دسترسی پیدا می‌کند) دسته بندی نمود.

۲-۲-۱-۲- دلایل بزه‌کاری

دلایل شامل دلایل اجتماعی (شامل محیط[۶۱]، ناسازگاری اجتماعی، تعارض نقش محول و محقق[۶۲] ، بی ثباتی شخصیتی و...) ، اقتصادی (فقر و بی کاری، کسب مال، رقابت ناسالم مالی و...)، سیاسی (مبارزه با سانسور، مقابله با مخالف، کنترل تحریک مخالفان، مبارزه با نظام حاکم و...) علمی و آموزشی (بررسی سطح مهارت، عدم وجود آزمایشگاه مجازی، رقابت علمی،عدم امکانات فنی سیستم‌ها و عدم امنیت در آنها و...)، روانشناختی (حسادت، جلب توجه و احساس حقارت و ارضا آن، غرور، احساس شکست ناپذیری،کنجکاوی، خشم و عصبانیت و هیجان، انتقام و... و یا اختلالات یا بیماری های روانی: اختلالات شخصیتی، اسکیزوفرنی، اختلال عاطفی دوقطبی، پرخاشگری، افسردگی، و...)،حقوقی (عدم ضمانت اجراهای مناسب، مشکلات پلیس و تعقیب و کشف و...) می‌باشد.

۲-۲-۲- بزه‌دیده

دسترسی غیرمجاز، سیستم‌ها و داده‌های رایانه‌ای را به عنوان هدف، مورد تعرض قرار می‌دهد. از این تهاجم، صاحبان و دارندگان آنها متحمل خسارات می‌گردند. نتیجه دسترسی غیر مجاز نسبت به هدف را دستیافتگی یا دستیابی و نسبت به صاحبان آنها را بزه‌دیدگی ناشی از دسترسی غیرمجاز می‌نامیم.

۲-۲-۲-۱- انواع بزه‌دیدگان

بزه‌دیدگان را می‌توان از نظر نوع (شامل اشخاص حقیقی: فرد یا گروهی از افراد و اشخاص حقوقی: خصوصی: شرکت‌ها و سازمان‌ها و... یا دولتی یا عمومی: سازمان‌ها، نهادها، شرکت‌ها و...)، سطح دانش (کم بهره یا بی بهره از دانش فنی و مهندسی خصوصاً علوم رایانه‌ای یا بهره‌مند از دانش مزبور [۶۳]، سطح امکانات (کم بهره از امکانات فنی و تجهیزاتی مناسب و کارآمد در تامین امنیت)، تعاملات اجتماعی (افرادی که زودباور و طبیعتاً ساده اندیش می‌باشند و به سادگی بر اساس یک روش کارای مهندسی اجتماعی مغلوب می‌گردند یا افراد سهل انگار یا بی احتیاط)، جامعه شناختی یا جرم شناختی (فرد یا گروه‌های منحرف اولیه یا ثانویه: مانند بزه‌کاران اتفاقی یا به عادت که خود بزه‌دیده واقع می‌شوند یا فرد یا گروه‌های ناکرده بزه یا کاملاً سازگار)

۲-۲-۲-۲- دلایل بزه‌دیدگی

شامل دلایل روانی (شامل درونی[۶۴]: غرور، هیجان، کنجکاوی و... و بیرونی شامل تحریک منفی مانند تمسخر توهین و... یا مثبت مانند تبلیغات یا بیانات کاذب و...) اجتماعی (شامل: تشکیل گروه‌های محرک و جاذب، نقش یا پایگاه اجتماعی جذاب یا محرک و...) ، اقتصادی (شامل: فقر و عدم امکانات مادی و مالی مناسب، عدم قدرت تجهیر به امکانات مناسب فنی به دلایل مختلف مالی و..)، سیاسی (رقابت بدون مطالعه با رقیب سیاسی، مبارزه طلبی نهادهای دولتی، تبلیغات یا فعالیت‌های مختلف علیه نظام حاکم و...)، علمی ـ آموزشی (شامل: کمی یا فقر علمی در حوزه فناوری اطلاعات و ارتباطات، عدم تخصص یا مطالعه علمی در دانش فنی و مهندسی و یا کارکرد سیستم‌ها و شبکه‌ها، عدم رعایت نکات امنیتی و ایمنی در سیستم‌ها یا بی‌توجهی یا بی‌احتیاطی در این خصوص و...)

۲-۲-۲-۳- آثار جرم بر بزه‌دیدگان

این آثار که شامل آثار منفی و مثبت و نسبت به اشخاص اعم از حقیقی و حقوقی می‌باشد، شامل: آثار روانی (به شکل منفی درونی شامل: عصبانیت، هیجان و اضطراب و دلهره، آشفتگی‌های حافظه و تمرکز حواس، سرخوردگی و بیرونی شامل: انتقام، تمسخر، توهین و افترا و سایر رفتارهای انحرافی با شکل اولیه یا ثانویه[۶۵])، اقتصادی (به شکل منفی شامل: تحمیل هزینه‌های پیش‌بینی نشده مالی در قالب هزینه‌های پیشگیری از جرم وکنترل وضعی، کاهش بازده و سود مالی شغلی مانند شرکت‌ها و...و به شکل مثبت شامل: ایجاد امنیت شغلی مرتبط با فناوری ارتباطات و اطلاعات و کسب درآمد بیشتر در درازمدت به دلیل هزینه‌های کنترل وضعی و...)، اجتماعی (به شکل منفی شامل تشکیل خرده فرهنگ منحرف[۶۶]، نابهنجاری، تعارض یا اختلال در نقش‌های اجتماعی، اختلال در سازگاری اجتماعی و.... به شکل مثبت شامل تشکیل گروه‌های حامی و مددرسان و...)، جرم‌شناختی (شامل اثر منفی به شکل بزه‌کاری موقت و به عادت) سیاسی (به شکل منفی در قالب مبارزه متقابل سیاسی، اقدام علیه نهادهای متولی فناوری اطلاعات و ارتباطات دولتی به شکل انتقام به اشکال مختلف و...)، آموزشی– علمی (به شکل منفی شامل مجهز شدن به برنامه‌های مخرب، یادگیری برخی از جرائم رایانه‌ای، انجام رقابت ناسالم با بزه‌کاران به جهت ارضا روانی، تشکیل کلاس‌های آموزشی جرائم رایانه‌ای، تشکیل گروه‌های ناسالم و منحرف در حوزه فناوری اطلاعات

و ارتباطات و... و به شکل مثبت شامل تجهیز شدن به دانش امنیت سیستم‌ها و شبکه‌ها و یا مطالعه تخصصی در علوم رایانه‌ای، تجهیز به ابزارهای نرم‌افزاری و سخت‌افزاری دفاعی و کنترل وضعی، تشکیل کلاس‌های امنیت سیستم‌ها و روش‌های مقابله با حملات رایانه‌ای، تشکیل گروه‌های دفاعی و همکاری و همیاری در حوزه فناوری اطلاعات و ارتباطات و...) می‌باشد.

۲-۲-۲-٤- حمایت از بزه‌دیدگان

در قالب حمایت‌های روحی ـ روانی (جهت کاهش آثار روانی ناشی از بزه یا ترمیم آن) حمایت اجتماعی (به شکل تشکیل گروه‌های واکنش سریع یا حمایت کننده یا پیشگیرانه)، اقتصادی (کمک‌های مادی یا مالی به افراد کم‌بهره از امکانات فنی، تأمین هزینه‌های مالی تجهیز به دانش فنی و مهندسی، ایجاد صندوق‌های حمایت‌کننده یا جبران‌کننده مستقیم خسارات، اعطای تسهیلات و...) حقوقی (به شکل پاسخ‌های مناسب و کارآمد در برابر بزه چه به شکل سرکوبگر: کیفری، انضباطی و غیر سرکوبگر: تدابیر پیشگیرانه رسمی یا جامعوی و چه به شکل جبران خسارات و مسئولیت مدنی).

۳- پاسخ‌های کیفری در برابر دسترسی غیرمجاز

در این قسمت از میان انواع پاسخ‌ها (شامل پاسخ‌های سرکوبگر و غیر سرکوبگر) تنها به بیان پاسخ‌های کیفری در برابر پدیده دسترسی غیرمجاز می‌پردازیم این پاسخ‌ها را در دو بعد حقوق داخلی ایران و حقوق بین‌الملل (نهادها، سازمان‌ها، اسناد بین‌المللی و نیز حقوق داخلی کشورها) مورد اشاره قرار خواهیم داد.

۳-۱- پاسخ‌ها ی کیفری در حقوق ایران

پاسخ‌های کیفری در حقوق ایران از نظر قوانین و مقررات و پیش نویس‌ها و رویه قضایی قابل بررسی می‌باشد که ذیلاً به بررسی آنها می‌پردازیم.

۳-۱-۱- پاسخ‌های کیفری در آیینه قوانین و مقررات

در قوانین جزایی اعم از مجموعه قانون مجازات اسلامی و سایر قوانین جزایی پراکنده دیگر، هیچ ماده قانونی در خصوص دسترسی غیرمجاز، به چشم نمی‌خورد؛ زیرا، اصولاً در مجموعه قوانین جزایی ایران تا کنون به جرائم رایانه‌ای پرداخته نشده. در بررسی قوانین جزایی سنتی چنین نتیجه‌گیری می‌شود که در برخی از آنها دسترسی غیرمجاز به عنوان یکی از شیوه‌های ارتکاب و در برخی دیگر به عنوان یک عامل تسهیل کننده محسوب می‌شود:

به عنوان مثال می‌توان به مواد ۵۰۱ (در خصوص در اختیار قراردادن اسناد) ۵۰۳ (در خصوص دخول به مواضع برای جاسوسی) ۵۰۵ (در خصوص جمع‌آوری اطلاعات طبقه بندی شده) ۵۰۶ (بی مبالاتی منتهی به تخلیه اطلاعاتی) و نیز مواد ۶۷۷ (تخریب اشیا) و ۶۸۷ (تخریب یا خرابکاری در تأسیسات و وسایل عمومی) از قانون مجازات اسلامی و مواد ۲۴(در خصوص جاسوسی)، ۹۳(در خصوص تخریب وسایل ارتباطی و مخابراتی و الکترونیکی) و ماده ۱۳۱(در خصوص تغییر یا حذف یا افشا اطلاعات رایانه‌ای) از قانون مجازات جرائم نیروهای مسلح و نیز ماده ۲۳ از قانون حمایت حقوق مؤلفان و مصنفان و هنرمندان، ماده ۱ از قانون رفع تجاوز از تأسیسات أب و برق کشور، ماده ۱ از قانون مجازات اخلال‌گران در تأسیسات آب و برق و گاز و مخابرات کشور، قانون مجازات اخلال‌گران در صنایع، ماده ۱ از قانون کیفر بزه‌های مربوط به راه آهن، بند یک از ماده واحده قانون مجازات اخلال‌کنندگان در امنیت پرواز هواپیما و خرابکاری در وسایل و تأسیسات هواپیمایی اشاره نمود.

۳-۱-۲- پیش‌نویس طرح‌ها و لوایح

پیش‌نویس‌های یاد شده شامل پیش‌نویس طرح قانونی جرائم رایانه‌ای، پیش‌نویس لایحه قانونی جرائم رایانه‌ای می‌باشد که ذیلاً به بررسی آنها می‌پردازیم.

۳-۱-۲-۱- پیش‌نویس طرح قانون جرائم رایانه‌ای [۶۷]

پیش‌نویس طرح قانون جرائم رایانه‌ای به جرائمی همچون کلاهبرداری رایانه‌ای، جعل رایانه‌ای، جاسوسی رایانه‌ای، تخریب و اخلال‌گری (سابوتاژ) رایانه‌ای، دستیابی و شنود غیرمجاز رایانه‌ای می‌پردازد به موجب ماده پیشنهادی در پیش‌نویس طرح قانونی جرائم رایانه‌ای دسترسی غیرمجاز چنین جرم‌انگاری شده است:

« هرکس عمداً و به طور غیرمجاز به داده‌ها، اطلاعات، برنامه‌ها و سیستم‌های رایانه‌ای و مخابراتی با یا بدون نقض تدابیر ایمنی و حفاظتی دستیابی پیدا کند، مرتکب دستیابی غیرمجاز شده و به زندان از سه ماه تا دو سال و جزای نقدی از یک میلیون تا ۱۰ میلیون ریال محکوم خواهد شد.»

بر اساس این پیش‌نویس:

اولاً، دسترسی غیرمجاز مقید به سیستم‌های ایمن و نیز نقض تدابیر ایمنی نشده است.

ثانیاً، از عنوان دستیابی غیر مجاز استفاده شده است.

ثالثاً، در کنار داده از اطلاعات، برنامه و سیستم‌های رایانه‌ای صحبت شده است.

۳-۱-۲-۲- پیش‌نویس لایحه قانونی جرائم رایانه‌ای [۶۸]

پیش‌نویس این لایحه که در کمیته مبارزه با جرائم رایانه‌ای شورای عالی توسعه قضایی تدوین شده است جرائمی را مورد اشاره قرار داده است از جمله:

کلاهبرداری رایانه‌ای، جعل و استفاده از داده‌های مجعول، شنود غیر مجاز، دسترسی غیر مجاز، تخریب و اختلال در داده‌های رایانه‌ای، اختلال در عملکرد سیستم رایانه‌ای، ممانعت در دستیابی به داده یا سیستم‌ها و...

بر اساس ماده ۴ از پیش‌نویس لایحه قانونی یاد شده:

«هر کس عمداً و بدون مجوز با نقض تدابیر حفاظتی سیستم یا داده‌های رایانه‌ای یا مخابراتی به آنها دسترسی یابد به جزای نقدی تا شش میلیون ریال یا به حبس تا یک سال محکوم می‌گردد.»

بر اساس این پیش‌نویس:

اولاً، دسترسی غیر مجاز مقید به سیستم‌های ایمن و نیز نقض تدابیر ایمنی شده است

ثانیاً، آماج سیستم و داده قرارداده شده است

ثالثاً، سیستم‌های غیر ایمن و نیز دسترسی بدون نقض تدابیر ایمنی از شمول ماده مزبور خارج می‌باشد.

۳-۱-۳- پاسخ‌های کیفری در آیینه رویه قضایی

همانگونه که بیان شد مجموعه قوانین جزایی ایران تا کنون به جرائم رایانه‌ای عموماً و دسترسی غیرمجاز خصوصاً، نپرداخته است. لذا محاکم در برخورد با چنین رفتارهایی با خلاء قانونی مواجه‌اند و از نظر اصولی چاره‌ای جز صدور قرار منع تعقیب یا عدم پیگرد به دلیل جرم نبودن فعل ندارند. با این حال در برخی از جرائم رایانه‌ای، برخی محاکم کوشیده‌اند، خلاء

قانونی را با قوانین سنتی جبران نمایند. این جرائم عموماً جرائمی می‌باشند که رایانه به عنوان ابزار یا وسیله ارتکاب مورد استفاده واقع می‌شوند.

در خصوص دسترسی غیرمجاز، از آنجایی که از دسته جرائم رایانه‌ای محض، تلقی می‌شود و با توجه به اینکه جرائم رایانه‌ای محض جرم‌انگاری نشده‌اند و امکان صدور حکم با قوانین سنتی نیز، وجود ندارد نتیجتاً، صدور حکم محکومیت فاقد وجاهت قانونی است. با این حال در خصوص جرائم مرتبط با رایانه از جمله کلاهبرداری رایانه‌ای، برخی معتقدند در مواردی که نتیجه جرم به صورت تحصیل وجه یا مالی می‌باشد ممکن است بتوان با توجه به ماده ۲ از قانون تشدید مجازات مرتکبین ارتشا و اختلاس و کلاهبرداری تحت عنوان تحصیل مال از طریق نامشروع حکم محکومیت صادر نمود.[۷۰]

۳-۲- پاسخ‌های کیفری بین‌المللی

یکی از دلایل جرم‌انگاری جرائم رایانه‌ای خصوصاً دسترسی غیر مجاز در قوانین ملی کشورها فشارهای بین‌المللی خصوصاً نهادها و سازمان‌های بین‌المللی در قالب توصیه نامه‌ها، توافق‌نامه‌ها و... می‌باشد که نهایتاً منجر به تصویب کنوانسیون جهانی جرائم محیط سایبر در بوداپست گردید.

۳-۲-۱- پاسخ‌های کیفری در اسناد بین‌المللی

در این قسمت، ابتدا پاسخ‌های مقدماتی کیفری از سوی نهادها و سازمان‌های بین‌المللی در برابر جرائم رایانه‌ای، خصوصاً دسترسی غیرمجاز را بیان می‌داریم و سپس به صورت اختصاصی به بررسی کنوانسیون جهانی بوداپست خواهیم پرداخت.

۳-۲-۱-۱- پاسخ‌های کیفری مقدماتی نهادها و سازمان‌های بین‌المللی

اقدامات اولیه را می‌توان اقدامات سازمان توسعه و همکاری اقتصادی، شورای اروپا، سازمان ملل، انجمن بین‌المللی حقوق جزا و سازمان پلیس بین‌الملل به عنوان پاسخ مقدماتی ذکر نمود.

۳-۲-۱-۱-۱- اقدامات سازمان توسعه و همکاری اقتصادی (OECD)

اولین اقدام بین‌المللی جامع در مورد برخورد با جرائم رایانه‌ای، به وسیله سازمان توسعه و همکاری اقتصادی انجام شد. از سال ۱۹۸۳ تا ۱۹۸۵ کمیته‌ای منتخب از سازمان مزبور امکان هماهنگی بین‌المللی را در زمینه قوانین کیفری بر علیه جرائم اقتصادی رایانه‌ای مورد بررسی قرارداد. در سپتامبر ۱۹۸۵ کمیته مزبور لیست اعمالی را پیشنهاد نمود که دسترسی یا شنود عمدی و بدون مجوز شخص مسئول سیستم جزئی از آن بود.[۷۱]

۳-۲-۱-۱-۲- اقدامات شورای اروپا

پس از ارائه لیست ECD ، شورای اروپا، مسأله جرائم رایانه‌ای را از دیدگاه تخصصی‌تر مورد مطالعه قرار داد و رهنمودهایی را به قانون‌گذران ملی ارائه داد یکی از بخش‌های شورای اروپا کمیته اروپایی ناشی از جرم است. مسأله جرم رایانه‌ای در سال‌های۸۶ – ۱۹۸۵ میلادی، در برنامه کار کمیته مزبور واقع شد. کمیته مزبور نیز کمیته‌ای تخصصی‌تر را برای بررسی تشکیل داد. این کمیته کار خود را در ۱۹۸۹ به پایان رساند و یک گزارش و یک توصیه‌نامه به کمیته اروپایی مشکلات ناشی از جرم ارائه کرد. در نهایت در سپتامبر ۱۹۸۹ پیشنهاد نهایی به کمیته وزرای شورای اروپا ارسال شد. پیشنهاد مزبور شامل دو لیست حداقل و اختیاری بود. دسترسی غیرمجاز در لیست حداقل آورده شده بود و این توجه ویژه شورای اروپا را به دسترسی غیرمجاز نشان می‌دهد. در بند «ه» از لیست یاد شده، دسترسی بدون حق به سیستم یا شبکه رایانه‌ای به وسیله تجاوز به تدابیر و ابزارهای امنیتی، مورد اشاره قرار گرفته است.[۷۲]

۳-۲-۱-۱-۳- اقدامات سازمان ملل

در دوازدهمین اجلاس عمومی کنگره هشتم که در ۱۹۹۰ برگزار شد، نماینده دولت کانادا پیش‌نویس قطعنامه‌ای را در مورد جرائم رایانه‌ای از طرف ۲۱ عضو حامی آن تسلیم کنگره نمود و کنگره در سیزدهمین اجلاس عمومی، قطعنامه مزبور را بعد از اصلاح پذیرفت. در این قطعنامه، پیشنهاداتی به کشورهای عضو شده است که دسترسی غیرمجاز از آن جمله می‌باشد. [۷۳]

۳-۲-۱-۱-٤- اقدامات انجمن بین‌المللی حقوق کیفری

در سال ۱۹۹۰ یکی از موضوعاتی که انجمن مزبور مطرح نمود، موضوع جرائم رایانه‌ای و سایر جرائم در قلمرو انفورماتیک بود. در سال ۱۹۹۲، نشست مقدماتی این بحث در دانشگاه ورتسبورگ آلمان انجام شد. همزمان با این نشست، سازمان ملل، جامعه اروپا و شورای اروپا نیز جلسات مشترکی در همین مورد منعقدکردند. نتیجه کار انجمن، چاپ کتابی ویژه جرائم رایانه‌ای و همچنین صدور قطعنامه‌ای حاوی فهرست جرائم رایانه‌ای بود. در سال ۱۹۹۴ نشست نهایی انجمن در «ریودوژانیرو» بود که ضمن تأیید لیست حداقل و لیست اختیاری شورای اروپا توصیه شد برخی از این جرائم مورد بازنگری قرار گیرند تا چند جرم دیگر نیز به لیست افزوده شود.[۷۴]

۳-۲-۱-۱-۵- اقدامات اینترپول

سازمان پلیس جنایی بین‌المللی، جرائم رایانه‌ای را تقسیم بندی نموده است که دسترسی غیرمجاز جزئی از آن می‌باشد این سازمان دسترسی غیرمجاز را شامل نفوذ غیرمجاز، شنود غیرمجاز و سرقت زمان رایانه‌ای دانسته است.[۷۵]

۳-۲-۱-۲- کنوانسیون جرائم محیط سایبر (بوداپست)

در ۱۹ سپتامبر ۲۰۰۱ ، معاونان وزرای شورای اروپا، کنوانسیون جرائم محیط سایبر را تصویب نمودند و کمیته وزرای شورای اروپا در ۸ نوامبر ۲۰۰۱ آن را تصویب نمود. کنوانسیون جرائم محیط سایبر در ۲۳ نوامبر ۲۰۰۱ در یک کنفرانس بین‌المللی که در بوداپست برگزار شد، برای امضا عرضه گشت. ۳۰ دولت، کنوانسیون را امضا نمودند: ۲۶ کشور ازاعضای شورای اروپا و۴ دولت غیرعضو که درتهیه پیش‌نویس کمک کرده بودند آن را امضا نمودند (کشورهای ژاپن، ایالات متحده، کانادا وافریقای جنوبی)[۷۶]

۳-۲-۱-۲-۱- ساختار کنوانسیون

این کنوانسیون در ۴۸ ماده و در ۴ فصل می‌باشد. فصل اول، در بیان اصطلاحات می‌باشد و فصل دوم، به بیان معیارهایی که می‌بایست در سطح ملی رعایت شود، شامل: موضوعات اصلی تشکیل دهنده حقوق کیفری و قوانین مربوط به آیین‌دادرسی و موضوع صلاحیت‌ها می‌باشد. فصل سوم، به بیان همکاری‌های بین‌المللی، شامل: اصول کلی (اصول مربوط به همکاری بین‌المللی، اصول راجع به استرداد مجرمین، اصول کلی راجع به همکاری دو جانبه، ارائه اطلاعات به طور داوطلبانه) و مقررات ویژه (همکاری دو جانبه در خصوص اقدامات موقت، همکاری دوجانبه در راستای اختیارات پی جویی) و فصل چهارم، به مقررات نهایی اشاره دارد. شامل: مراحل امضا و لازم الاجرا شدن کنواسینون و الحاق به کنوانسیون، اجرای در حوزه تحت قلمرو، آثار کنوانسیون، اعلامیه‌ها.

۳-۲-۱-۲-۲- جرائم مورد اشاره در کنوانسیون

بخش اول از فصل دوم کنوانسیون، به بیان موضوعات اصلی تشکیل دهنده حقوق کیفری می‌پردازد. در این بخش، جرائمی که می‌بایست در حوزه قوانین ملی کشورها جرم‌انگاری شوند، مقرر شده است. این جرائم، خود در سرفصل‌هایی تقسیم‌بندی شده‌اند که شامل: جرائم علیه محرمانگی و تمامیت و در دسترس بودن سیستم‌ها و داده‌های رایانه‌ای، جرائم مرتبط با رایانه، جرائم مرتبط با محتوا، جرائم مرتبط با تعرض به حق نشر و حقوق مربوط به آن می‌باشد. در جرائم علیه محرمانگی و تمامیت و در دسترس بودن سیستم‌ها و داده‌های رایانه‌ای جرائمی همچون: دسترسی غیرمجاز، قطع و شنود غیر مجاز، ایجاد اختلال در داده‌ها ایجاد، ایجاد اختلال در سیستم‌ها، سوء استفاده از دستگاه‌ها اشاره شده است. در جرائم مرتبط با رایانه جرائمی همچنون جعل رایانه‌ای و کلاهبرداری رایانه‌ای مورد اشاره قرار گرفته و در جرائم مرتبط با محتوا جرائم مرتبط با هرزه نگاری کودکان مورد توجه قرار گرفته است .

۳-۲-۱-۲-۳- دسترسی غیر مجاز در کنوانسیون

بر اساس ماده دوم از عنوان اول از بخش اول از فصل دوم کنوانسیون جرائم محیط سایبر:

«هر یک از اعضا، باید به گونه‌ای اقدام به وضع قوانین و مقررات نمایدکه در صورت لزوم، بر اساس نیازهای حقوق داخلی خود، هر نوع دسترسی عمدی من غیر حق را به تمام یا قسمتی از سیستم رایانه‌ای خود یک فعل مجرمانه تلقی کند. ممکن است عضو مورد نظر مقرر دارد که جرم در اثر تعرض به سیستم‌های ایمن، با قصد دسترسی به داده‌های رایانه‌ای یا دیگر مقاصد ناروا یا نسبت به سیستم رایانه‌ای که با سیستم رایانه‌ای دیگری در ارتباط می‌باشد محقق می‌شود.»[۷۷]

بر اساس این ماده:

اولاً، به مفهوم عام دسترسی غیر مجاز توجه شده است.

ثانیاً، دسترسی غیر مجاز به سیستم‌های رایانه‌ای اختصاص یافته.

ثالثاً، به دسترسی مقید در مقام دادن اختیار به کشورها در نوع جرم‌انگاری توجه شده است.

۳-۲-۲- پاسخ های کیفری در برخی از کشورها

در بررسی قوانین جزایی برخی از کشورهای جهان چنین دریافت می‌شود که برخی از این کشورها از عنوان«هکینگ» استفاده و هر نوع تغییر، تخریب، افشا، کسب داده، بررسی سیستم و... را به عنوان مصادیق آن بیان نمودند. به عنوان مثال می‌توان به قانون فناوری اطلاعات هند فصل ۱۱ بند۶۶ اشاره نمود که به حذف، تغییر، هر نوع تأثیر زیان‌آور به داده‌های موجود در سیستم با قصد خاص اشاره دارد و یا قانون جزایی آلمان بند الف ۲۰۲ که به کسب غیر مجاز داده‌های حفاظت شده پرداخته می‌توان اشاره نمود.

برخی دیگر دسترسی غیرمجاز بدون قید یا قصد خاص جرم انگاری نموده‌اند منتهی آماج را گاه، داده‌های رایانه‌ای قرار داده‌اند و گاه سیستم‌ها. به عنوان مثال می‌توان به قانون مصون بودن از افشاء اطریش مصوب سال ۲۰۰۰ یا ماده ۲۶۳ قانون جزای دانمارک یا ماده ۳۰۷ج بند ۲قانون جزایی یونان یا ماده۴ قانون رایانه اسرائیل یا ماده ۲۱۱ بخش ۹ فصل دوم قانون جزا مکزیک یا ماده ۲ از قانون جرائم پردازش داده‌ها به طور خودکار به شماره ۱۹/۲۲۳ شیلی اشاره نمود که در تمام موارد به دسترسی غیرمجاز به داده‌های رایانه‌ای اشاره دارد. همچنین می‌توان به ماده ۱-۵۰۹ فصل ششم قانون مورخ جولای ۱۹۹۳ در

رابطه با تقویت مبارزه علیه جرائم مالی و رایانه‌ای لوکزامبورگ یا ماده ۱۳۸الف قانون جزای هلند اشاره نمود که به دسترسی غیرمجاز به سیستم‌های رایانه‌ای اشاره دارد.

برخی دیگر دسترسی غیرمجاز را مقید به قصدهای خاص نموده‌اند. به عنوان مثال می‌توان به ماده ۱ از بند ب مواد۵۵۰ بخش ۵ از قانون جزایی جرائم رایانه بلژیک اشاره نمود.

برخی دسترسی غیرمجاز به سیستم‌ها را مقید به ایمن بودن دانسته‌اند و برخی چنین قیدی را لازم ندانسته‌اند به عنوان مثال می‌توان به ماده ۸ از فصل ۳۸ قانون جزایی فنلاند یا ماده ۶۱۵ قانون جزایی ایتالیا یا ماده ۱۴۳ مکرر قانون جزا سوییس اشاره نمود که به دسترسی غیرمجاز به سیستم‌های حفاظت شده پرداخته‌اند.

برخی دسترسی غیرمجاز به سیستم‌ها را به قصد دسترسی به داده‌های خاص جرم‌انگاری نموده‌اند. به عنوان مثال می‌توان به ماده ۱-۳۴۲ از قانون جزایی کانادا یا ماده ۲۷ قانون مخابرات هنگ‌کنگ اشاره نمود.

برخی از کشورها نیز علاوه بر دسترسی غیرمجاز باقی ماندن در سیستم یا حفظ دسترسی غیرمجاز به سیستم را جرم‌انگاری نموده‌اند به عنوان مثال می‌توان به ماده ۱-۳۲۳ فصل سوم قانون جزایی جدید فرانسه یا ماده ۶۱۵ قانون جزایی ایتالیا اشاره نمود.

برخی از کشورها در خصوص دسترسی غیرمجاز به گونه‌ای کاملاً فنی و تکنیکی به ذکر جزئیات سطح دسترسی غیرمجاز به سیستم‌ها پرداخته‌اند مانند بند ۲ از ماده ۳ از قانون دسترسی غیرمجاز به رایانه قانون شماره ۱۲۸سال ۱۹۹۹ ژاپن [۷۸]

☑ عنوان: جرایم مرتبط با محتوا: محتوای سیاه فناوری اطلاعات

☑ نویسنده: آقای حسن عالی‌پور

(دانشجوی دکترای حقوق جزا و جرم شناسی دانشگاه شهید بهشتی و مدرس دانشگاه)

چکیده

جرایم مرتبط با محتوا، عنوانی جدید از برخی جرایم است که به تبع شکل‌گیری حقوق کیفری فناوری اطلاعات در مباحث حقوقی و سیاهه‌های قانون، نمود یافته است. جرایم مرتبط با محتوا ناظر به جرایمی است که در فضای مجازی رایانه و اینترنت از طریق محتویات غیرقانونی علیه اشخاص یا عفت و اخلاق و آسایش عمومی ارتکاب می‌یابد. این محتویات که عمدتاً به شکل تصویر، صوت یا نوشته هستند، ماهیتاً غیرقانونی، بی ارزش و غیرقابل حمایت هستند و نمود آنها در فضای مجازی رایانه یا اینترنت بیانگر وقوع جرم یا اعمال خلاف اخلاق است. در جرایم مرتبط با محتوا، سیستم رایانه‌ای و فضای اینترنت، وسیله ارتکاب جرم است اما برخلاف سایر جرایم رایانه‌ای در این قسم از جرایم، داده محتوا که جزیی از دادهٔ رایانه‌ای محسوب می شود، نه وسیله ارتکاب جرم است و نه هدف آن، بلکه نفس داده محتوا، غیرقانونی است که یا باید محو شود یا اصلاح گردد. جرایم مرتبط با محتوا دارای اقسام مختلفی است که از جمله می‌توان به هرزه‌نگاری اشخاص، هرزه‌نگاری شخصیت، توهین و افترا، آموزش ارتکاب جرایم یا فعالیت‌های خطرناک، نشر اکاذیب و ... اشاره کرد.

واژه‌های کلیدی: داده محتوا، داده رایانه‌ای، اطلاعات رایانه‌ای، فضای سایبر، محتویات غیرقانونی.

۱- مقدمه

تحولات شگفت انگیز فناوری اطلاعات در اوایل قرن بیست و یکم، دو پیامد مهم را به دنبال داشته است: یکی تغییر دنیای واقعی و دیگری ترسیم دنیای مجازی. در دنیای واقعی، صنعت انفورماتیک و فناوری اطلاعات در تمام شؤون زندگی مردم رخنه کرده است، به گونه‌ای که هر فرد در زندگی روزمره خود به طور ملموس از ظهور صنعت انفورماتیک متأثرمی شود. رایانه ای شدن فعالیتها و تسریع در تبادل اطلاعات تا اندازه زیادی بار افزایش بی رویه جمعیت و بالا رفتن نیازها و توقعات انسانها را بر دوش می‌کشد و فراتر از این در سطح جامعه، فناوری اطلاعات دستاویزی برای پیشرفت، تأمین رفاه افراد جامعه و تعامل بیشتر با سایر جوامع است. از این حیث فناوری اطلاعات در دنیای واقعی به دنبال متحقق ساختن سه هدف عمده است:

الف) ایجاد تعامل بیشتر بین جوامع و جهانی شدن ارتباطات و فناوری اطلاعات

ب) دیجیتالی کردن کلیه فعالیت‌های اصلی روزمره و در نتیجه انجام سریع خواسته‌های روزمره بشری و به تبع آن تـأمین رفـاه بیشتر.

ج) کم کردن فاصله موجود در بین کشورهای پیشرفته و کشورهای در حال توسعه از حیث تبادل اطلاعات و فراهم نمودن یـک جامعه بین‌المللی یک دست. اینها مظاهری از تغییرات بنیادین فناوری اطلاعات در دنیای واقعی است. امـا شـگفتیهای فنـاوری اطلاعات به همین جا ختم نمی‌شود و عجیب‌تر آنکه فناوری اطلاعات دنیای جدیدی را با نام دنیای مجازی، رایانه و ا ینترنت یا فضای سایبر خلق کرده است. دنیای جدید کلاً با دنیای واقعی متفاوت است. انسانها نمی‌توانند به طور ملموس وارد آن شوند اما از طریق آن می‌توانند کلیه مکانها را در نوردند و فارغ از قید و بندهای زمان، با کلیهٔ سرزمینهای ایـن دنیـای تـازه متولـد شـده ارتباط برقرار کنند. شبکه جهانی اینترنت مصداق برجسته این دنیای مجازی است که در آن اطلاعات با کمیت غیر قابل تصور و با سرعتی باور نکردنی مبادله می‌شوند. به این دنیا، مخابرات و سیستم‌های رایانه‌ای محلی و منطقـه‌ای را نیزبایـد اضـافه کـرد. مجموعاً برای شناسایی و درک دنیای مجازی اینترنت و رایانه درتقابل با دنیای واقعی می‌توان به موارد زیر اشاره کرد:

۱-۱- فضای مجازی رایانه و اینترنت دارای مالک مشخصی نیست و قابلیت تملک ندارد:

دنیای سایبر یا فضای مجازی رایانه و اینترنت دارای مالک مشخصی نیست و همانند دنیای واقعی، محیطی است برای اسـتفاده تمامی انسانها با این تفاوت که دنیای واقعی اولاً مخلوق انسان نیست و ثانیاً اسـتفاده از آن بـدون وجـود امکانـات بـرای همـه انسانها میسر است ،اما دنیای مجازی رایانه و اینترنت مخلوق انسان است و استفاده از آن منوط به وجود برخی امکانات مادی و معنوی است. هر چند دنیای مجازی، مخلوق اندیشه انسانهاست اما گویی بشر در قبال دنیای سایبر دست به یک کشـف بـزرگ زده است تا یک اختراع خارق‌العاده. از این حیث این کشف بزرگ، برکتی برای کلیه انسانهاست تا بتوانند در راستای زندگی بهتر از آن استفاده کنند. نتیجتاً عدم وجود مالک مشخص برای فضای سایبر یا عدم تملک این فضا، به معنای عدم نظارت و کنتـرل بر آن نیست و بلکه چنین دنیایی همانند دنیای واقعی باید تحت کنترل و نظارت در بیاید تا از آسیب دشمنان آن در امان بمانـد .قابل ذکر است که در سال ۱۹۹۲، یک گروه غیر انتفاعی با عنوان " جامعه اینترنت " تشکیل یافته است که شکل‌گیری قوانین اینترنت و پروتکل هایی که نحوه استفاده و ارتباط با اینترنت را تعیین می‌کنند، مورد بازبینی قرار می‌دهد.[۱]

۱-۲- فضای مجازی رایانه و اینترنت مفاهیم زمان و مکان را دگرگون ساخته است.

فضای سایبر، دنیای اذهان است که از طریق سیستم رایانه‌ای و اینترنتی نمود می‌یابد. ایـن دنیـای جدیـد از دام زمـان و مکان رسته است: از دام زمان از این حیث که در کوتاهترین زمان ممکن، اطلاعات، مبادله می‌شوند و داده‌ها، پردازش می‌شوند و به همین ترتیب ،جرایم رایانه‌ای در مدت بسیار کوتاهی در مکانهای متفاوتی ارتکاب می‌یابند و از دام مکان از این جهـت کـه استفاده از محیط رایانه و اینترنت امکان برقراری ارتباط به کلیه مکانها را فراهم مـی‌سـازد و ایـن سـیر و سـیاحت از مکانهـای مجازی در مدت زمان بسیار اندکی میسر است. به همین دلیل فضای رایانه و اینترنت زمان و مکان را بـه هـم نزدیـک سـاخته است و به میزان غیر واقعی کردن این دو، جرایم ارتکابی در محیط سایبر نیـز معـادلات کیفـری تـابع زمـان و مکـان از قبیـل صلاحیت کیفری، زمان وقوع جرم و ... را برهم زده است.

۱- مجله اینترنت، سال دوم، شماره هشتم، اردیبهشت و خرداد ۱۳۸۳،ص ۶

۱-۳- فضای مجازی رایانه و اینترنت، فضای آزادیهاست.

دنیای جدید، موقعیتی را به وجود آورده است که افراد، فارغ از هر گونه نظارت و کنترل در خلوت خود در مقابل رایانه قرار بگیرند و به راحتی وارد فضای افسار گسیخته‌ای شوند که اثری از عوامل دولتی و جامعوی محدود کننده آزادی نیست. به همین منوال افراد با آزادی کامل قدم در جای جای فضای سایبر می‌گذارند و چه بسا مرتکب افعالی شوند که در دنیای واقعی هرگز نتوانند یا نخواهند که این افعال را انجام دهند. اگر با رویکرد مقررات کیفری موجود در دنیای واقعی به فضای رایانه و اینترنت بنگریم، به این نتیجه نایل می‌شویم که فضای سایبر چقدر مجرم‌پرور است و حال آنکه مقایسه این دو دنیا اساساً اشتباه است. فضای سایبر، فضای اذهان است. همانقدر که افراد در اذهان خود می‌توانند مرتکب هر فعل یا ترک فعل مجرمانه‌ای بشوند، در محیط اینترنت و رایانه تا هنگامی که به دیگری ضرری وارد نسازند، می‌توانند آزاد باشند. پس آزادی، لازمه فضای سایبر است اما این آزادی، افسار گسیخته نیست. در فضای سایبر این آزادیها تا جایی پیش می‌رود که متضمن ورود ضرر به اشخاص یا جامعه نگردد، در غیر این صورت به عنوان یک جرم با مرتکب آن برخورد خواهد شد.

۱-٤- فضای مجازی رایانه و اینترنت، بیانگر جلوه‌هایی از سرشت پلید انسان است.

در مواجهه با این بحث فلسفی که سرشت انسان بر پلیدی است یا انسان بر فطرت پاک آفریده شده وراه به سوی نیکی و خیر دارد، فضای سایبر می‌تواند موضع‌گیری به جهتی داشته باشد که در آن جهت انسان راه به سوی پلیدی دارد. فرد در فضای سایبر که مالک مشخصی ندارد و از دام زمان و مکان رسته است و فضای آزادیهاست، عملاً از سر کنجکاوی، غریزه شهوت‌طلبی یا حس زیاده‌خواهی و شرارت، مرتکب اعمالی می‌شود که یا قانوناً جرم یا اخلاقاً مذموم است. مراجعه همگانی به سایتهای غیرمجاز، تصاویر هرزه و محتویات شهوت‌انگیز بیانگر این است که غریزه انسانها به طور طبیعی راه به سوی این محتویات یا سایتها دارد و کنترلهای قهرآمیز دولتی یا اجتماعی یا ترس از آبروریزی در نزد افراد اجتماع، عامل اصلی انحراف غرایز انسان از مسیر طبیعی در فضای واقعی است. در کشوری چون آمریکا که ایجاد روابط جنسی به یک امر عادی در محیط واقعی تبدیل شده و از قید محدودیتها رهایی یافته است، کلمه سکس بیشترین کلمه‌ای است که در اینترنت جستجو می شود؛ ۲۵ میلیون آمریکایی از مجموع افرادی که به اینترنت دسترسی دارند در هر هفته بین یک تا ده ساعت، وقت برای مراجعه به سایتهای غیرمجاز یا سایتهای جنسی صرف می‌کنند و ۶۰ درصد از صفحات اینترنتی که مورد مراجعه قرار می‌گیرند، سایتهای جنسی است.[۲] حال در جوامعی که نظارت و کنترل بر فعالیتهای جنسی یا روابط بین زن و مرد شدید است، این ارقام و درصدها افزایش چشمگیری می‌یابند.

به هر حال دنیای مجازی اینترنت و رایانه یا فضای سایبر با موقعیتها و شرایطی که دارد، باید درک شود تا در برخورد سرکوبگر و کیفری با جرایم ارتکابی در این فضا، سیاست کیفری افتراقی اتخاذ گردد. این سیاست کیفری در حقوق کیفری رایانه‌ای در مقایسه با مقررات کیفری دیگر از این حیث افتراقی خواهد بود که به آزادیها و گرایشهای انسان در خلوتشان توجه دارد و این موضوع مخصوصاً در جرایم مرتبط با محتوا نمود بیشتری می‌یابد. جرایم مرتبط با محتوا که محصول داده محتواهای نامشروع و غیرقانونی در فضای سایبر است، از حیث تنوع و تکثر نسبت به سایر جرایم رایانه‌ای، در اولویت قرار دارد و قسمت اعظم این

۲- به نقل از روزنامه همشهری، شماره ۳۱۹۸، شنبه ۲۶ مهر ۱۳۸۲،ص ۲

جرایم در محیط واقعی قابل ارتکاب نیست، چه این جرایم که هرزه‌نگاری مصداق برجسته آن است، در نتیجه آزادی و تمایلات سرشت انسان در محیط مجازی اینترنت و رایانه ارتکاب می‌یابند و چاره‌ای جز این نیست که واقعیت این جرایم را پذیرفت، از حذف کامل آنها دل کند و در اتخاذ سیاست کیفری نسبت به آنها واقع بین بود. جرایم مرتبط با محتوا ارتباط تنگاتنگ با آزادی، خلوت و تمایلات حیوانی انسان دارند که به لحاظ اینکه در محیط واقعی در زیر ذره بین کنترل و نظارت دولتی و اجتماعی قرار دارند، در فضای سایبر و صنعت فناوری اطلاعات بیشتر نمود می‌یابند.

۲- شناسایی جرایم مرتبط با محتوا

شناسایی جرایم مرتبط با محتوا با توجه به اینکه اصطلاح کاملاً جدیدی است به دو طریق صورت می‌گیرد: نخست از طریق تعریف این اصطلاح و دوم از لحاظ علل انتخاب این عنوان. محتوا معادل واژه Content است و به طور شفاف و دقیق در سیستم رایانه‌ای و اینترنتی از واژه‌هایی همچون داده (Data) و اطلاعات (Information) متمایز نگشته است.[۳] بنابراین قبل از شناسایی محتوا یا داده محتوا باید مفهوم داده و اطلاعات شناخته شوند. داده رایانه‌ای هر نمادی از وقایع، اطلاعات، اشکال یا مفاهیم است که قابل ایجاد یا ارایه یا انتشار یا پردازش در سیستم رایانه‌ای باشد. اوصاف عمده داده رایانه‌ای را می‌توان به این صورت بیان کرد که: اولاً لزوماً متضمن بیان مفهوم یا اطلاعات قابل درک نیست و ایجاد یک خط یا نقطه یا حرف به معنای ایجاد یا ارایه داده خواهد بود. ثانیاً همواره دارای ارزش مالی نیست و بلکه بسیاری از داده‌های رایانه‌ای دارای ارزش اقتصادی نبوده و قابلیت داد و ستد ندارند که عموماً این نوع از داده‌ها را می‌توان بر دو قسم، تقسیم بندی کرد:

الف) داده‌های نامفهوم و ناکارآمد: داده‌هایی هستند که به طور جداگانه بیانگر اطلاعات یا مفاهیم قابل درک نیستند و به تنهایی قابلیت پردازش یا استفاده در سیستم رایانه‌ای ندارند مانند یک نقطه یا یک حرف.

ب) *داده‌های غیرقانونی:* داده‌های هستند که به لحاظ ماهیت مجرمانه‌اشان صرفاً در راستای اهداف و مقاصد غیرقانونی به کار می‌آیند و استفاده مجاز و قانونی در محیط سایبر از آنها ممکن نیست؛ مانند محتویات مستهجن یا محتویات متضمن هتک حرمت و افترا. ثالثاً همیشه در مرئی و منظر کاربر سیستم رایانه‌ای یا استفاده کننده از آن قرار نمی‌گیرد؛ به این معنی که عملکرد سیستم رایانه‌ای از آن حیث که در محیط مجازی قرار دارد جز با داده‌های رایانه‌ای میسر نیست و داده رایانه‌ای چه

۳- فرهنگ تشریحی کامپیوتر میکروسافت بدون تفکیک شفاف و دقیق واژه‌های داده، اطلاعات و محتوا، آنها را اینگونه تعریف می‌کند Data (داده) جمع لاتین لغت Datum، به معنای یک قلم از اطلاعات است. در عمل، لغت "داده" هم به صورت جمع و هم به صورت مفرد به کار می‌رود.Information (اطلاعات) به معنای داده‌ها به شکلی که مردم تفسیر می‌کنند. داده از حقایقی تشکیل شده که وقتی درعمل مفهومی را به گیرنده برسانند، عنوان " اطلاعات " را می‌گیرند. رایانه‌ها بدون درک معنای اطلاعات، آنها را پردازش می‌کنند. Content (محتوا) ، داده‌ای است که بین دنباله‌های ابتدایی وانتهایی یک عنصر در سند HTMLیاSGML ظاهر می‌شود. محتوای یک عنصر ممکن است متن ساده یا عناصر دیگر باشد. همچنین به محتوا بدنه پیام یک عنوان گروه خبری یا پیام پست الکترونیک نیز می‌گویند. (فرهنگ تشریحی کامپیوتر مایکروسافت ۲۰۰۳، ترجمه حسنوی، رضا و فرسایی، داریوش، انتشارات دانشیار، ویرایش پنجم، تهران، چاپ اول، پاییز ۱۳۸۱، ص ۱۳۷، ۱۵۴، ۲۹۸) ملاحظه می‌شود که فرهنگ مزبور نیز نتوانسته یا نخواسته است تا بین اصطلاحات مورد بحث تفکیک قائل شود. حتی مقرر کرده است که داده یک قلم از اطلاعات است و درجایی دیگر مقرر می‌دارد که اطلاعات، داده‌های دارای مفهوم هستند و قاعدتاً در این دو تعبیر مشخص نیست که اطلاعات عام تر از داده است یا داده عام‌تر از اطلاعات.

آشکار و چه به صورت پنهان، عمل پردازش یا سایر فعالیت‌های مربوطه را انجام می‌دهد. قسمتهای زیادی از این فعالیتها هرگز بر صفحه رایانه آشکار نمی‌شود و از این حیث، تشخیص جرایم ارتکابی علیه آنان یا از طریق آنان که به جرایم پنهان محیط سایبر(Hiding Crimes) مشهور هستند، بسیار مشکل است.

اطلاعات رایانه‌ای عبارت است از داده، متن، تصویر، صدا، کد، پایگاه داده، هر گونه نرم افزار ایجاد شده یا قابل انتقال یا ذخیره در سیستم رایانه‌ای است که بیانگر واقعیت قابل درکی باشند. با توجه به این تعریف به نظر می‌رسد که اطلاعات رایانه‌ای عام‌تر از داده رایانه‌ای باشد. اما باید گفت در تفکیک این دو اصطلاح اختلاف نظر وجود دارد؛ از یک طرف می‌توان گفت که داده‌های ناکارآمد و نامفهوم متضمن هیچگونه اطلاعاتی نیستند و نتیجتاً اطلاعات محسوب نمی‌شوند و از سوی دیگر می‌توان ادعا داشت که کد یا صدا یا امواج مغناطیسی یا حتی پایگاه داده در زمره اطلاعات محسوب می‌شوند و حال آنکه اطلاق داده بر آنها بدون اشکال نیست. به همین دلیل در فضای سایبر عزم جدی در تفاوت‌گذاری نسبت به این دو اصطلاح وجود ندارد و غالباً به جای همدیگر استعمال می‌شوند. با توجه به توضیحات فوق، محتوا یا داده محتوا، نسبت به داده و اطلاعات مفهوم خاص‌تری دارد. محتوا ناظر به پیکربندی داده‌ها یا اطلاعات رایانه‌ای است که حالتی گسترده تر و کلان‌تر نسبت به آنها دارد.[۴] محتوا در واقع مضمون داده‌ها و اطلاعات است از آن حیث که اولاً از طریق پردازش داده رایانه‌ای ایجاد می‌شود ثانیاً به نحو غالب ناظر به تصویر یا صوت یا نوشته است که نتیجتاً قابل دیدن و شنیدن به وسیله انسان هستند، به عنوان مثال یک تصویر از منظره طبیعی یا یک عکس از انسان در سیستم رایانه‌ای، داده محتوا محسوب می‌شود که از طریق داده رایانه‌ای، پردازش شده و مضمون و معنای مشخصی از داده را ارایه می‌کند. این داده محتوا ممکن است قانونی باشد یا غیرقانونی و غیرقانونی بودن محتوا یا ناظر به ذات محتوا است یا ناظر به فعل محتوا. محتوای غیرقانونی ذاتی، محتوایی است که صرفاً در راستای اهداف غیرقانونی و نامشروع یا در راستای ارتکاب جرم ایجاد یا ذخیره یا ارایه می‌گردد که خصیصه برجسته آن بی ارزش و غیر اقتصادی بودن است؛ مانند محتویات هرزه یا محتویات متضمن توهین یا افترا. محتوای غیرقانونی فعلی، محتوایی است که عملکرد آن عموماً یاجرم است یا برای ارتکاب جرایم رایانه‌ای به کار می‌آید. با این خصیصه که این قسم از محتویات رایانه‌ای ذاتاً بی‌ارزش و ناکار آمد نیستند و به طور قانونی نیز می‌توان از آنها استفاده کرد؛ مثل ویروس‌ها یا کرم‌های رایانه‌ای.جرایم مرتبط با محتوا (content Related crime) اصطلاح جدیدی است که پس از تصویب کنوانسیون جرایم محیط سایبر بوداپست در سپتامبر ۲۰۰۱ (که فصل ۳ این کنوانسیون با عنوان «جرایم مرتبط با محتوا» متمایز شده است) به طور رسمی و فراگیر وارد حقوق کیفری کشورهای جهان شد. جرایم مرتبط با محتوا مولود حقوق کیفری رایانه‌ای است که البته کلاه برخی از جرایم ارتکابی در محیط واقعی را بر سر کرده است و اگر از عنوان جرایم مرتبط با محتوا و محدوده آن بگذریم، تقریباً در زیر مجموعه مباحث مربوط به جرایم مرتبط با محتوا، با جرایم سنتی مواجه هستیم.

جرایم مرتبط با محتوا را می توان به طور خاص و عام تعریف کرد: جرایم مرتبط با محتوا در مفهوم خاص عبارت است از جرایمی که از طریق محتویات غیرقانونی علیه عفت یا اخلاق عمومی یا سلامت جسمی یا روانی اشخاص یا شخصیت معنوی آنان ارتکاب می یابد. در این تعریف، رکن مادی جرایم در محیط سایبر تحقق می‌یابد اما آثار آن در محیط خارجی نمود پیدا می‌کند؛ مثل توهین یا افترا نسبت به دیگری از طریق سیستم رایانه‌ای. جرایم مرتبط با محتوا در مفهوم عام شامل جرایمی

۴- یکی از دو تعریف فرهنگ تشریحی کامپیوتر مایکروسافت به نوعی مؤید این تعریف است. در این فرهنگ آمده است که محتوا، داده‌ای است که بدنه پیام یک عنوان گروه خبری یا پیام پست الکترونیکی را تشکیل می‌دهد .

می‌شود که در آنها داده محتوا یا وسیله ارتکاب جرم است مثل محتویات متضمن ویروس رایانه ای یا داده محتوا، هدف جرم قرار می‌گیرد؛ مثل تخریب یا جعل محتویات رایانه‌ای و یا اینکه به معنای دقیق کلمه نه وسیله ارتکاب جرم است و نه هدف آن و بلکه به صورت ماهیت نامشروع و غیرقانونی در می‌آید و اثرات خود را در محیط خارجی بروز می‌دهد. در این حالت از یک طرف محتویات غیرقانونی، وسیله ارتکاب جرم نیستند؛ زیرا با تحقق و عینیت یافتن این محتویات چه به صورت ایجاد و چه به صورت انتشار یا ارایه یا ذخیره، جرم تحقق یافته است و در واقع وسیله اثرگذاری بر جامعه یا اشخاص خارج از محیط سایبر است. از طرف دیگر محتویات غیرقانونی هدف مجرم نیستند؛ چون ماهیتاً بی‌ارزش و غیرقانونی و در نتیجه غیرقابل حمایت هستند و به لحاظ همین خصیصه جرم علیه آنها صورت نمی‌پذیرد و در این جا هدف جرم جامعه یا اشخاص خارج از سیستم رایانه‌ای هستند. به هر حال محتویات غیرقانونی نفساً و ذاتاً جرم محسوب می‌شوند، مشروط بر اینکه موضوع افعالی چون تولید، انتشار، ذخیره، ارایه و .... قرار بگیرد و وجود این محتویات بر صفحه رایانه حکایت از ایجاد و انتشار آنها داشته و گویای وقوع جرایم مرتبط با محتوا خواهد بود. در نتیجه منظور از جرایم مرتبط با محتوا در این تحقیق جرایم مرتبط با محتوا در مفهوم خاص است.

جرایم مرتبط با محتوا عمدتاً جرایم یا انحرافات جنسی یا جرایم علیه عفت و اخلاق عمومی را به ذهن متبادر می‌سازد اما باید گفت از یک طرف جرایم مرتبط با محتوا را نمی‌توان جرایم جنسی یا جرایم مرتبط با جنسیت دانست؛ چون در فضای سایبر جرم جنسی تحقق نمی‌پذیرد و بلکه عناوین مجرمانه مربوط به ارایه یا انتشار محتویات مربوط به جرم جنسی یا عمل جنسی است که در این فضا تحقق می‌یابد. مضافاً این که برخی از جرایم مرتبط با محتوا مانند نشر اکاذیب، افترا، توهین به مقدمات و .... ارتباطی به جرایم یا امور جنسی ندارند. از طرف دیگر بحث از جرایم مرتبط با محتوا در زیر مجموعه جرایم علیه عفت و اخلاق عمومی صحیح نیست , چون برخی از جرایم مرتبط با محتوا مانند نشر تصاویر خانوادگی یا اسرار خصوصی دیگری بدون رضایت وی و یا نشر اکاذیب اصولاً ارتباطی با اخلاق و عفت عمومی ندارد و حتی جنبه خصوصی آنها بر جنبه عمومی غلبه داشته و جزء جرایم قابل گذشت محسوب می‌شوند و همین طور جرایم علیه شخصیت معنوی افراد نیز برای جرایم مرتبط با محتوا ناقص خواهد بود؛ چه تولید یا انتشار محتویات مستهجن داخل در این قسم نخواهند بود. با این وصف، عنوان «جرایم مرتبط با محتوا» یا جرایم محتوایی عنوان کم نقص و مناسبی است که می‌توان در قبال برخی از جرایم رایانه‌ای به کار برد و آن را به محیط سایبر منصرف ساخت.

۳- اقسام جرایم مرتبط با محتوا

ماده ۹ کنوانسیون جرایم محیط سایبر از میان جرایم مرتبط با محتوا، فقط به هرزه نگاری اشخاص زیر ۱۸ سال اشاره کرده است و حال آن که محدوده جرایم مرتبط با محتوا بسیار فراتر از هرزه‌نگاری است. جرایم مرتبط با محتوا شامل جرایم تصویری، صوتی و نوشتاری در سیستم رایانه‌ای و اینترنتی است که ذیلاً مصادیق آن ذکر می‌شود:

الف- هرزه‌نگاری اطفال و بزرگسالان

ب - هرزه‌نگاری و تحریف انگاری هویت

ج – هتک حرمت (شامل قذف، افترا و توهین)

د- اهانت به مقدسات مذهبی

هـ- دعوت یا تحریک یا تشویق یا تهدید اطفال به ارتکاب جرایم

و - آموزش جرایم یا فعالیتهای خطرناک

ز – آموزش افکار و عقاید خطرناک یا گمراه کننده
ح – نشر اکاذیب
ط – تولید یا انتشار محتویات نفرت‌انگیز یا نژادپرستانه
ی – تهدید و اذیت و آزار دیگری
ک – توریسم جنسی

جرایم فوق که تحت عنوان محتویات غیرقانونی و عموماً در قالب نوشته یا تصویر یا صوت ارتکاب می‌یابند در یک خصیصه مشترک‌اند و آن جنبه غیرقانونی بودن، بی‌ارزش بودن و عدم قابلیت داد و ستد در بین مردم است؛ چه این محتویات یا باید از بین بروند و یا اصلاح گردند و الا کاربرد قانونی و عقلانی از طرف آنها متصور نیست.

غیر از جرایم فوق، برخی جرایم دیگر را نیز به لحاظ برخی شباهتها می‌توان در زمره جرایم مرتبط با محتوا ذکر کرد؛ مانند ارسال نامه‌های اینترنتی ناخواسته یا افشاء یا انتشار محتویات یا اسرار خصوصی. در ارسال نامه‌های اینترنتی ناخواسته که در برخی کشورها همچون انگلستان جرم انگاری شده است، محتویات مندرج در رایانامه ممکن است ذاتاً نامشروع و غیرقانونی باشد یا اینکه قانونی و مباح باشد؛ مانند قطعاتی از اشعارگوته یا حافظ که در اینجا دریافت‌کننده رایانامه مایل به دریافت آنها نیست. در افشاء یا انتشار محتویات یا اسرار خصوصی، تصویر، نوشته یا صوت که در قالب محتوا در سیستم رایانه‌ای نمود یافته‌اند، بدون رضایت صاحب آنها انتشار می‌یابند یا در دسترس دیگران قرار می‌گیرند.این محتویات نه تنها ذاتاً غیرقانونی نیستند، بلکه مورد حمایت قانون قرار گرفته‌اند.جرایم مرتبط با محتوا که در بالا به آنها اشاره شد یا دارای سابقه تقنینی هستند یا فاقد سابقه قانونگذاری بوده و به اقتضای سیستم رایانه‌ای به وجود آمده‌اند و یا اینکه سابقه تقنینی داشته و لیکن در محیط سایبر با عناوین متفاوت یا با شرایط مختلف مطرح می‌شوند. بنابراین در تطبیق جرایم مرتبط با محتوا با عناوین مجرمانه در قوانین و مقررات جزایی ایران سه حالت قابل تصور است. الف) برخی از جرایم مرتبط با محتوا در مقررات جزایی سابقه قانونگذاری دارند و سیستم رایانه‌ای در قبال ارتکاب این قسم از جرایم، در حد وسیله ارتکاب جرم مطرح می‌شود؛ مانند قذف، توهین، افترا و اهانت به مقدسات مذهبی که بر اساس قانون مجازات اسلامی و به ترتیب در مواد ۵۱۳،۶۹۷،۶۰۸،۱۰۴ و ۵۱۴ قابل مجازات شناخته شده‌اند. پس هر کس از طریق سیستم رایانه‌ای محتوای متضمن قذف، توهین یا افترا را تولید کند یا انتشار دهد یا در دسترس دیگران قرار دهد. به نحوی که جرایم فوق ارتکاب یابند، مرتکب بر اساس مواد قبل‌الذکر مجازات خواهد شد.

ب) برخی از جرایم مرتبط با محتوا سابقه قانونگذاری نداشته و در قوانین و مقررات جزایی انعکاس نیافته‌اند. علت فقدان سابقه تقنینی این قسم از جرایم یا به دلیل کم اهمیت بودن آنها در محیط واقعی است و یا اینکه به اقتضای سیستم رایانه‌ای و سریع تر شدن تبادل اطلاعات مطرح شده‌اند؛ مانند ارسال نامه‌های اینترنتی ناخواسته یانفرت انگیز، انتشار اسرار یا محتویات خصوصی، ترویج ایدئولوژی‌های خطرناک و ..

ج) برخی از جرایم مرتبط با محتوا سابقه تقنینی داشته ولی به لحاظ عدم کارآیی یا تکافوی مقررات سنتی یا اقتضای شرایط مربوط به محیط اینترنت از حیث جزایی فاقد سابقه تقنینی هستند و باید نسبت به آنها اقدام به وضع قانون کرد؛ مثلاً نشر اکاذیب بر اساس ماده ۶۹۸ قانون مجازات اسلامی جرم است اما وسایل ارتکاب این جرم در ماده مربوطه به صورت حصری ذکر شده است که به لحاظ عدم تکافوی این ماده یا ابهامی که ممکن است از خصیصه حصری بودن آن ظهور نماید،

جرم‌انگاری آن در فضای سایبر ضروری می‌نماید و یا با توجه به آزاد بودن محیط رایانه و اینترنت و عدم امکان تهدید آزادی یا حیثیت افراد در این فضا به شکلی که در محیط خارج متصور است، باید دیگاهها را نسبت به جرم‌انگاری محتویات مستهجن و مبتذل تعدیل کرد و در فضای سایبر مقررات متفاوتی نسبت به آنها وضع کرد.

٤- جرم‌انگاری اعمال غیرقانونی مرتبط با محتوا

جرم انگاری در فضای سایبر از جهات مختلف با جرم‌انگاری در فضای واقعی متفاوت است . فارع از مبانی واصول جرم انگاری در فضای واقعی مثل ایجاد گزاره های اخلاقی و ایراد ضرر به دیگری برخی مسائل دیگر نیز باید مد نظر قرار بگیرد که بی توجه به آنها نمی توان جرم انگاری مناسب و مؤثر داشت .

برای جرم‌انگاری نسبت به اعمال غیرقانونی و غیراخلاقی محتوای رایانه ای باید به مسائل پنجگانه زیر توجه داشت:

۴-۱- مسائل مربوط به مرتکب جرم: در جرایم مرتبط با محتوا که عموماً حول محور امور مرتبط با جنسیت و هرزه‌نگاری می‌چرخد، مجرم شخصی است که به اقتضای غرایز حیوانی‌اش که توأم با آزادی و خلوت وی در فضای سایبر است، مرتکب جرم شده است. در این جا حتی می‌توان بحث جبرگرایی کیفری متعادل را پیش کشید که به موجب آن ارتکاب جرم مرتبط با محتوا کمتر تحت تأثیر اراده آزاد یا اختیار بوده است و با وجود این که این اراده آزاد نفی نمی‌شود ولی به طور جدی از عواملی همچون شرایط حاکم بر جامعه، تأثیر امیال و غرایز حیوانی، وجود محیطی عاری از نظارت و کنترل و... متأثر بوده است. بنابراین در اعمال خلاف قانون و اخلاق مرتبط با محتوا به ویژه اعمال مرتبط با جنسیت، مرتکب یک فرد سودانگار وحسابگر نیست و بلکه اراده‌اش عموما" تحت تأثیر عوامل درونی و بیرونی می باشد.

۴-۲- مسائل مربوط به بزه‌دیده جرم: بزه‌دیده جرایم مرتبط با محتوا همانند جرایم دیگر هم فرد است و هم جامعه . در همه جرایم فرض بر این می‌شود که جامعه از حیث معیارهایی چون امنیت، اعتماد، آسایش، عفت و اخلاق، بزه‌دیده واقع می‌شود و بنابراین تمام جرایم، جنبه عمومی پیدا می کنند. اما بر عکس در همه جرایم، بزه‌دیده فردی وجود ندارد و به همین دلیل برخی از جرایم دارای جنبه خصوصی نیستند. در هر حال در تمامی جرایم، جامعه و در اکثر جرایم، افراد به عنوان بزه‌دیدگان جرایم مطرح می‌شوند که بر حسب مستقیم یا غیر مستقیم بودن ضرر وارده، مجازات عمل ارتکابی چه از حیث قانون و چه از حیث قضاوت در نوسان است. در اکثر جرایم مرتبط با محتوا برخلاف سایر جرایم رایانه‌ای مانند کلاهبرداری، جعل، تخریب، جاسوسی و ... بزه‌دیدگی مستقیم وجود ندارد. توضیح اینکه در جرایم مرتبط با محتوا، بزه‌دیدگی از حیث جامعوی چندان ملموس نیست؛ چه هتک عفت و اخلاق عمومی در محیط سایبر که اکثر افراد جامعه در این فضا بر خط نیستند یا چنانچه مشغول استفاده از سیستم رایانه‌ای و اینترنتی هستند، می‌توانند از سایت غیرقانونی یا محتویات مجرمانه به راحتی چشم‌پوشی کنند، بسیار کم رنگ است و به آن غلظتی نیست که می‌توان در محیط واقعی تصور کرد. از حیث بزه‌دیدگی فردی نیز وجود رضایت بزه‌دیده در برخی از جرایم مرتبط با محتوا مانند هرزه‌نگاری، مداخله و تأثیر بزه‌دیده در وقوع جرم مثل از طریق برخط شدن و ارتباط با مرتکب و یا بی‌احتیاطی بزه‌دیده و مسائلی از این قبیل، جرم‌انگاری بی‌رویه و اعمال مسوولیت کیفری کامل نسبت به مرتکب جرایم مرتبط با محتوا را با تردید مواجه می‌سازد.

۴-۳- مسائل مربوط به موضوع جرم: موضوع جرم یا هدف جرم شخص یا چیزی است که جرم علیه آن ارتکاب می‌یابد. موضوعات جرایم مرتبط با محتوا بسیار گسترده است. حمایت از بسیاری از این موضوعات به لحاظ ابهام یا ورود در دایره گزاره های اخلاقی، عملاً محدود ساختن آزادی‌های فردی است. در محیط اینترنت و رایانه نمی‌توان با استناد به خلاف

عفت و اخلاق عمومی یا خلاف موازین شرعی، اقدام به جرم‌انگاری نسبت به محتویات نمود ؛ چه در اکثر مواقع چاره‌ای جز بستن اکثر قریب به اتفاق سایتها نخواهد بود. از سوی دیگر اگر در صدد آن بود که محتویات متضمن ایدئولوژی‌های خطرناک یا القای بدبینی و ایجاد یأس در مردم یا حتی محتویاتی با مضامین تبلیغ علیه نظام و سیاستهای آن را جرم‌انگاری کرد، در واقع چشم‌پوشی از واقعیتهای رایانه و اینترنت خواهد بود که از یک طرف فضای سایبر عملاً در مالکیت حکمرانان مستبد قرار خواهد گرفت و از طرف دیگر آزادیهای فردی حتی در خلوت افراد نیز خدشه‌دار خواهد شد. دو نتیجه‌ای که اصولاً با خصایص فضای سایبر یعنی عدم مالکیت نسبت به آن و تأمین محیط آزادیها منافات خواهد داشت .

۴-۴- مسائل مربوط به فرهنگ جامعه: جرایم مرتبط با محتوا تابع فرهنگ هر جامعه است و از این حیث در مقایسه با جرایم دیگر از حیث زمان و مکان به شدت در نوسان بوده و از مصادیق برجسته جرایم نسبی یا مصنوعی محسوب می‌شود. جرایم مرتبط با محتوا رابطه تنگاتنگی با آداب، رسوم، مذهب، عقاید و باورهای جوامع دارد و به همین دلیل مقررات جزایی کشورها در ارتباط با جرایم مرتبط با محتوا نسبت به همدیگر شباهتهای کمتری دارند؛ مثلاً بر اساس کنوانسیون جرایم محیط سایبر مصوب سپتامبر ۲۰۰۱، جرایم مرتبط با محتوا فقط منصرف به هرزه‌نگاری اشخاص زیر ۱۸ سال است که آن هم عمدتاً به صورت تصویر جنسی صریح مدنظر گردآورندگان کنوانسیون بوده است و حال آنکه طبق قانون حمایت خصوصی از اطفال استفاده کننده از اینترنت مصوب ۱۹۹۸ آمریکا، علاوه بر تصاویر و اصوات متضمن آمیزش جنسی اشخاص زیر ۱۸سال یا برهنگی آنها، ارایه یا انتشار هر محتوای شهوت‌انگیز نسبت به آنها جرم تلقی شده است. ملاحظه می‌شود که در جامعه آمریکا برای سلامت جنسی، جسمی و روحی اطفال و نوجوانان، از الفاظ مبهم و کش داری چون «شهوت‌انگیز» استفاده شده است. در کشور ما به لحاظ تأثیر مذهب و فرهنگ بومی، قاعدتاً دایرهٔ جرایم مرتبط با محتوای وسیع‌تر می‌شود و به عنوان مثال در قبال هرزه‌نگاری، جامعه ما حاضر به تفکیک بین هرزه‌نگاری اطفال و بزرگسالان نیست و هرزه‌نگاری هر دو را مورد نکوهش قرار می‌دهد. به هر حال جرایم مرتبط با محتوا با توجه به فرهنگ و مذهب و مقررات و قوانین کشور نمود می‌یابد و به همین دلیل در ارتباط با این جرایم، تقلید و الگوبرداری از مقررات جزایی سایر کشورها عملاً بلاطائل است.

۴-۵- مسائل مربوط به قانونگذاریهای سابق: برای جرم‌انگاری نسبت به جرایم مرتبط با محتوا با توجه به تکثر و تنوع آنها باید به قانونگذاریهای سابق نیز توجه داشت؛چه ممکن است مقنن سابق، برخی از جرایم مرتبط با محتوا را در قالب قوانین و مقررات جزایی دیگر پیش‌بینی کرده باشد و به لحاظ اینکه فضای سایبر یا رایانه در این قبیل جرایم در حد وسیله ارتکاب جرم است لزومی به جرم‌انگاری مجدد احساس نمی شود. در ارتباط با جرایم مرتبط با محتوا، قوانین جزایی سابق ممکن است سه حالت داشته باشند:

الف) برخی از جرایم مرتبط با محتوا در قوانین جزایی سابق پیش‌بینی نشده‌اند و علت این امر در این است که این قسم از جرایم یا صرفاً با فضای سایبر معنا می‌یابند یا این که وقوع آنها در محیط خارجی بنا به برخی ملاحظات مدنظر مقنن قرار نگرفته‌اند، ولی در محیط اینترنت و رایانه به لحاظ سرعت تبادل اطلاعات و محتویات , قانونگذار لازم دانسته است تا نسبت به آنها جرم‌انگاری کند. برای این حالت می‌توان به جرایم آموزش ارتکاب جرم برای اشخاص زیر ۱۸ سال، افشا یا انتشار و اسرار خصوصی، نشر اکاذیب و... اشاره کرد.

ب) برخی از جرایم مرتبط با محتوا در مقررات جزایی پیش‌بینی شده‌اند اما در فضای مجازی رایانه یا اینترنت لازم است یا محدوده آنها توسعه یابد و یا برعکس باید حیطه آنها محدود گردد ؛ به عنوان مثال در ارتباط با توسعه محدوده جرم‌انگاری

نسبت به مقررات جزایی سابق می‌توان به تبصره ۳ ماده ۳ قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت‌های غیرمجاز می‌نماید مصوب ۲۴ بهمن ۱۳۷۲ مقرر می‌دارد که استفاده از صغار برای نگهداری، نمایش، عرضه، فروش و تکثیر نوارهای غیرمجاز موضوع این قانون، موجب اعمال حداکثر مجازاتهای مقرره برای عامل خواهد بود. در فضای اینترنت و رایانه به لحاظ خطرات بیشماری که اطفال را تهدید می‌کند، ضروری است که پا را فراتر گذاشته و تحریک یا تشویق یا تطمیع یا دعوت یا تهدید به دسترسی به محتویات غیر مجاز نیز جرم‌انگاری شود.

برعکس در ارتباط با تحدید حدود جرم‌انگاری نسبت به مقررات جزایی سابق در فضای سایبر می‌توان به ماده ۶۴۰ قانون مجازات اسلامی اشاره کرد که تجارت یا توزیع یا ساخت یا در معرض عمومی گذاردن هر چیز خلاف عفت و اخلاق عمومی را جرم‌انگاری کرده است و در واقع تفاوتی بین بزرگسالان و کودکان نیز قائل نشده است. اجرای این ماده در محیط اینترنت نه تنها عملاً غیرممکن است و منجر به بسته شدن اکثر سایتهای اینترنتی می‌شود بلکه با ماهیت و شرایط اینترنت نیز همخوانا نیست. به همین دلیل در فضای سایبر ضروری است که محتویات هرزه را محدود کرد و معیارهای کلی و مبهمی همچون خلاف عفت و اخلاق عمومی برای تشخیص محتویات هرزه را کنار گذاشت.

ج) برخی از جرایم مرتبط با محتوا جرایمی هستند که در مقررات جزایی انعکاس یافته‌اند و سیستم رایانه و اینترنتی وسیله‌ای مناسب برای ارتکاب آنهاست. لزومی به جرم‌انگاری این قبیل از جرایم نیست و با این که در دسته جرایم مرتبط با محتوا قرار می‌گیرند، بر اساس مقررات جزایی مربوطه قابل کیفر هستند؛ مثل افترا، توهین، هتک حرمت نسبت به مقدسات و ...

۵- جرایم مرتبط با محتوا در لایحه مجازات جرایم رایانه‌ای[۵]

فصل چهارم لایحه مجازات جرایم رایانه ای و از ماده ۱۵ تا ماده ۱۹ در ارتباط با جرایم مرتبط با محتوا است که ذیلاً به این مواد و دلایل توجیهی آنها اشاره می‌شود.

۵ـ۱ـ هرزه نگاری بزرگسالان

ماده ۱۵ مقرر می دارد: **«هر کس از طریق سیستم رایانه‌ای یا مخابراتی محتویات مستهجن از قبیل نمایش اندام جنسی زن و مرد یا نمایش آمیزش یا عمل جنسی انسان یا انسان با حیوان را تولید کند یا منتشر سازد یا مورد هر قسم معامله قرار دهد، به حبس از نود و یک روز تا یک سال یا پرداخت جزای نقدی از دو میلیون و پانصد هزار تا ده میلیون ریال و یا به هر دو مجازات محکوم خواهد شد».**

تبصره ۱: چنانچه محتویات موضوع این ماده در دسترس اشخاص زیر ۱۸ سال تمام قرار داده شود یا برای آنها منتشر یا ارائه گردد مرتکبین به حداکثر یک یا هر دو مجازات مقرر محکوم خواهند شد.

تبصره ۲: تولید محتویات غیر واقعی (از قبیل پویا نمایی، طراحی و نقاشی) با قصد انتشار یا معامله مشمول مقررات این ماده است.

۵-لایحه مجازات جرایم رایانه‌ای در دو قسمت ماهوی و شکلی در کمیته مبارزه باجرایم رایانه‌ای شورای عالی توسعه قضایی تدوین یافته است. تحقیقات مقدماتی این لایحه از زمستان ۱۳۸۱ آغاز ومراحل کارشناسی آن در بهار ۱۳۸۳ خاتمه یافت .مسئولیت نگارش است برخی از مواد این لایحه برعهده نگارنده بوده است که مواد ۱۵ تا۱۹ از جمله آنهاست .

توجیه اصلی قانونگذاری در راستای جرم تلقی کردن تولید یا انتشار یا مورد معامله قرار دادن محتویات هرزه، دفاع از عفت و اخلاق جامعه است. تولید و انتشار انبوهی از تصاویر یا اصوات مستهجن که اکنون در فضای مجازی اینترنت و مخابرات شایع است، به شدت سلامت اخلاق اشخاص و بویژه اطفال را تهدید می‌کند. تصاویری که برخلاف موازین عقلی و شرعی بوده و مذاق جنسی را متنوع ساخته و آثار زیانباری در روابط خارجی افراد می‌گذارد و به نوعی می‌توان گفت که فضای آلوده سایبر محدود به صندلی مقابل صفحه رایانه یا لحظه‌ای که کاربر از اینترنت استفاده می‌کند، نیست و بلکه این فضا روزنه تزلزل اخلاق جمعی در فضای واقعی است[۶] و به همین دلیل فضای سایبر باید از گزند محتویات منافی عفت و اخلاق عمومی در امان باشد. این ماده بر اساس حمایت از اخلاق فردی و جمعی تدوین یافته و جرم موضوع آن در زمره جرایم غیر قابل گذشت است. این ماده سابقه تقنینی در کشورهای پیشرفته از حیث اینکه در آن کشورها نسبت به بزرگسالان آزادی جنسی برقرار است، ندارد و مقررات این ماده فراتر از مقررات این کشورها و کنوانسیون بوداپست و منطبق بر فرهنگ ایران نگاشته شده است.

با التفات به نسبی بودن بسیاری از موضوعات و مصادیق اخلاقی و فرهنگی و تغییر و تبّدل مداوم آنها و با درک مقتضیات و مطلوبهای فضای سایبر که مفاهیم اساسی همچون آزادی، زمان، مکان، نظارت و ... در این فضا کلا متفاوت از مفاهیم مشابه در فضای واقعی است، محدودهٔ جرم‌انگاری موضوع ماده ۱۵ محدود به محتویات با مضمون نمایش اندام جنسی زن و مرد یا نمایش آمیزش یا عمل جنسی صریح بین انسان یا انسان با حیوان است. این محتویات اعم از تصاویر یا صوت است که ممکن است به اشتراک یا انفراد تولید یا منتشر شوند. تعیین مستهجن بودن تصویر با توجه به معیار مورد نظر در ماده آسان است اما تعیین استهجان صوت اگر تنها باشد یک امر قضایی است و قاضی یا بازپرس با استفاده از کارشناس بسته به وجود قراین و شواهد می‌تواند به این موضوع پی ببرد.

مضمون محتویات عبارتست از:

الف) اندام جنسی زن و مرد: منظور از اندام جنسی شامل اندام‌های برجسته‌ای در زن می‌شود که مرد فاقد آن است که شامل آلت تناسلی و پستانها است و در مردها نیز شامل یک اندام برجسته است وآن آلت تناسلی مردانه است. اندام جنسی علاوه بر اینها شامل مقعد و مجموعه باسن نیز می‌شود.

ب) نمایش آمیزش یا عمل جنسی انسان یا انسان با حیوان: منظور از آمیزش جنسی، فعل و انفعالات جنسی بین انسان (اعم از آمیزش جنسی بین دو یا چند زن و مرد و یا دو یا چند زن با هم و یا دو یا چند مرد با هم) یا انسان با حیوان است که ممکن است به صورت تصویر متحرک باشد و یا تصویر ثابت که حکایت از آمیزش داشته باشد. در آمیزش انسان با حیوان، انسان فقط فاعل آمیزش جنسی نیست و ممکن است مفعول واقع شود و به لحاظ اینکه حیوان شعور و آگاهی از این قبح فعل خویش ندارد، در واقع این انسان است که به صورت غیرطبیعی با حیوان، بهره جنسی می‌برد. تصاویر یا محتویات مربوط به آمیزش

۶- یکی از نویسندگان برجسته غربی با تاکید بر انبوه جرایم و وحشی‌گری‌هایی که اینترنت به نمایش می‌گذارد به طور طنز آمیزی مایل به استفاده از تعبیر "غرب وحشی وحشی Wild Wild West- به جای تعبیر " شبکه جهانی وب World Wide Web -" در قبال اختصار " w.w.w" است که در ابتدای هر پایگاه اینترنتی ذکر می‌شود (ر. ک به مقدمه کتاب مسئولیت ارایه‌دهندگان خدمات اینترنتی با مشخصات :
Timothy.D.casey:Isp Liability Survival Guide,Jhon vily and sons,may2000

جنسی حیوان با حیوان مشمول این ماده نمی‌شود. منظور از عمل جنسی، هرگونه رفتاری است کـه بـا نمـایش انـدام تناسـلی، بیانگر نوعی ارضای جنسی یا رفتار آشکار است که شخص با خود دارد که نمونه برجستهٔ آن خود ارضایی است.

ج- سایر موارد: تصاویر یا اصوات به عنوان محتویات مستهجن به صورت تمثیلی آورده شده اسـت. مـوارد تمثیلـی دیگـر بایـد همانند یا هم‌سنج مصادیق ذکر شده در ماده باشند و از این حیث محدوده مصادیق تمثیلی بسیار کم است؛ مـثلاً یـک تصـویر لخت که حاکی از آمیزش جنسی نباشد و اندام جنسی نیز دیده نشود در زمره این مصادیق تمثیلی است.رکن مادی جرم موضوع ماده مورد بحث از اجزای زیر تشکیل می شود.

الف ـ رفتار مجرمانه: فعل فیزیکی یا رفتار مجرمانه جرم مورد بحث سه فعل است که هر کدام از آنها با تحقق شرایط دیگـر توصیف مجرمانه را شکل می‌دهد.

نخست: تولید کردن محتویات هرزه (محتویاتی با مضمون نمایش اندام جنسی زن و مرد یا نمایش آمیـزش یـا عمـل جنسـی صریح بین انسان یا انسان با حیوان و امثال آن) به معنای ساختن یا ایجاد کردن آنهاست خواه به صورت واقعـی و خـواه غیـر واقعی. اگر تولید در محیط خارج صورت گرفته باشد؛ مثل جائیکه در مکانی از یک زن برهنه عکس‌برداری شده باشد، مشـمول مادهٔ فوق نمی‌شود اما در جاییکه از طریق Web cam از یک آمیزش جنسی فیلم‌بـرداری مـی‌شـود و همزمـان در اینترنـت منتشر می‌یابد، عمل ارتکابی مشمول ماده مورد بحث است. قابل ذکر است که محتویات واقعی عمدتاً در محـیط واقعـی تولیـد می‌شوند و سپس در محیط اینترنت ارایه یا انتشار می یابد، اما محتویات غیـر واقعـی اعـم از کـارتونی، نقاشـی، دسـتکاری در تصاویر واقعی، انیمیشن و ... بیشتر در محیط سایبر تولید می‌شود و اگر در خـارج از محـیط سـایبر تولیـد شـوند، تولیـد کننـده براساس این ماده مجازات نمی‌شود.

دوم: انتشار دادن محتویات هرزه به معنای توزیع و پخش این محتویات در محیط سایبر است و تعداد کسانیکه نسـبت بـه آنهـا انتشار صورت می‌گیرد باید از سه نفر بیشتر باشند و عرفاً به آن انتشار اطلاق شود.

سوم: مورد معامله قرار دادن: محتویات هرزه باید در سیستم رایانه‌ای و اینترنتی، مورد معامله اعم از بیع، اجاره و هبه واقع شوند تا مشمول این ماده گردند و عرضه برای معامله یا در معرض نمایش گذاشتن برای هر قسم معامله اگر منطبق بر انتشار نباشـد، جرم موضوع این ماده تحقق نخواهد یافت و ممکن است در شروع به جرم باشد که البته شروع به جرم موضـوع ایـن مـاده، جرم محسوب نمی شود.

ب) وسیله ارتکاب جرم: جرم موضوع این ماده، یک جرم صرفاً سایبری یا مجازی است که از طریق سیسـتم رایانـه‌ای یـا مخابراتی ارتکاب می‌یابد. محتویات موضوع این ماده قانوناً بی‌ارزش هستند و به لحاظ همین بی‌ارزش و مستهجن بودن، جـرم علیه آنها صورت نمی‌گیرد بلکه جرم علیه عفت و اخلاق عمومی جامعه صورت می‌پذیرد و سیستم رایانه ای و مخابراتی، وسیله تولید، انتشار و معامله این محتویات است.

ج) مرتکب جرم: لفظ «هرکس» بیانگر این است که هر کس اعم از شخص حقیقی یا حقوقی می‌تواند مرتکب جرم موضـوع این ماده باشد و صاحب تصاویر مستهجن اگر خود مباشرت در این جرم کرده باشد از تحمل کیفر این ماده مستثنی نیست.

د) نتیجه مجرمانه: جرم موضوع این ماده مطلق است و صرف وقوع فعل فیزیکی با سـایر شـرایط دیگـر کفایـت مـی‌کنـد و حصول نتیجه مجرمانه شرط تحقق جرم نیست؛ چه این جرم به طور قطع نتیجه ملموسی نمی‌توانـد داشـته باشـد و بـه لحـاظ

هتک عفت عمومی باید به صورت مطلق باشد یا به عبارت دیگر هتک عفت و اخلاق عمومی در زمان ارتکاب جرم موضوع این ماده مفروض است.

هـ- رکن روانی : جرم تولید یا انتشار یا مورد معامله قرار دادن محتویات هرزه یک جرم عمدی است که سوءنیت عام آن قصد انجام افعال مجرمانه موضوع این ماده ؛ یعنی تولید محتویات هرزه، انتشار این محتویات و مورد معامله قرار دادن آنها است. وجود سوء نیت خاص شرط نشده است .

ز- مجازات : کیفر مقرر برای جرم تولید، انتشار یا مورد معامله قرار دادن محتویات هرزه با توجه به ماده ۶۴۰ قانون مجازات اسلامی و درک مقتضیات وشرایط فضای سایبر به صورت اختیاری یا حبس از ۳ ماه و یک روز تا یکسال است یا جزای نقدی از دو میلیون و پانصد هزار تا ده میلیون ریال یا هر دو مجازات است که قاضی با توجه به میزان محتویات هرزه و کیفیات آن و سابقه مرتکب می‌تواند مجازات متناسب را اتخاذ نماید.

تبصره ۱ ماده ۱۵ مقرر میدارد : چنانچه محتویات موضوع این ماده در دسترس اشخاص زیر ۱۸ سال تمام قرار داده شود یا برای آنها منتشر یا ارایه گردد، مرتکبین به حداکثر یک یا هر دو مجازات مقرر محکوم خواهند شد. این تبصره در راستای حمایت اطفال و اشخاص زیر ۱۸ سال در برابر تصاویر و محتویات مربوط به اشخاص بالاتر از ۱۸ سال است که انتشار یا در دسترس قرار دادن یا ارایه محتویات این ماده نسبت به آنها با حداکثر حبس یعنی یکسال یا حداکثر جزای نقدی یعنی ده میلیون ریال یا حداکثر هر دو مجازات مواجه است. اصطلاح «در دسترس قرار دادن» لفظ عامی است که شامل هر شکل ارایه یا فراهم نمودن دستیابی می‌شود که یکی از این اشکال، معامله محتویات هرزه با شخص زیر ۱۸ سال است. انتشار یا در دسترس قرار دادن باید همواره با علم و آگاهی مبنی بر اینکه دریافت کننده یک شخص زیر ۱۸ سال است، صورت بگیرد؛ به عنوان مثال با رایانامه محتویات هرزه برای طفل بفرستد یا سایت اختصاصی برای آنها افتتاح کند و الا انتشار به صورت عمومی یا در دسترس همگان قرار دادن حتی با این علم که اشخاص زیر ۱۸ سال نیز به آن دست خواهند یافت، از شمول تبصره یک این ماده خارج خواهد بود.

تبصره ۲ماده ۱۵ نیز اشعار می‌دارد که تولید محتویات غیر واقعی (از قبیل پویا نمایی، طراحی و نقاشی) با قصد انتشار یا معامله مشمول مقررات این ماده است.» تولید محتویات غیر واقعی به صورت کارتونی، انیمیشن، نقاشی، طراحی و .... که مجموعاً زیر مجموعه تصویر و فیلم هستند، اگر به قصد انتشار یا معامله نباشد جرم نیست؛ زیرا آن شخص این محتویات را یا برای خود تولید می‌کند یا برای دیگری، مشروط بر اینکه مصداق انتشار یا معامله نباشد. پس تولید محتویات هرزه غیر واقعی در صورتی بر اساس این ماده قابل کیفر است که به قصد انتشار یا معامله باشد یا عملاً مورد انتشار یا معامله واقع شود.

تولید محتویات واقعی به این معنا که از عملکرد جنسی واقعی انسان یا انسان با حیوان صورت بگیرد، اگر در محیط واقعی باشد بر اساس ماده ۶۴۰ قانون مجازات اسلامی و یا قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت‌های غیر مجاز می‌نمایند مصوب ۱۳۷۲/۱۱/۲۳ قابل کیفر است و اگر در اشکال نادر در محیط سایبر صورت بگیرد حتی اگر به قصد انتشار یا معامله هم نباشد بر اساس این ماده قابل کیفر است.

۵-۲- جرایم مرتبط با اشخاص زیر ۱۸ سال

ماده ۱۶ اشعار می دارد:« هر کس از طریق سیستم رایانه ای یا مخابراتی مرتکب اعمال زیر شود، در مورد جرایم موضوع بند الف به حبس از یک سال تا سه سال یا پرداخت جزای نقدی از ده میلیون تا سی میلیون ریال یا به هر دو مجازات و در مورد جرایم موضوع بند ب و ج به حبس از نود و یک روز تا یک سال یا پرداخت جزای نقدی از دو میلیون و پانصد هزار تا ده میلیون ریال یا به هر دو مجازات محکوم خواهد شد».

الف) محتویات مستهجن از قبیل نمایش اندام جنسی یا نمایش آمیزش یا عمل جنسی اشخاص زیر ۱۸ سال یا ظاهراً زیر ۱۸ سال تمام تولید یا ارایه یا منتشر یا ذخیره سازی یا تهیه یا در دسترس دیگران قرار دهد.

ب) به منظور دستیابی اشخاص زیر ۱۸ سال تمام به محتویات موضوع بند الف این ماده یا ماده قبل، مبادرت به تبلیغ یا تحریک یا تشویق یا دعوت یا فریب یا تهدید آنها نموده یا طریق دستیابی به محتویات مذکور را تسهیل نموده یا آموزش دهد.

ج) به منظور ارتکاب جرایم و انحرافات جنسی یا سایر جرایم یا خودکشی یا استعمال مواد روانگردان اشخاص زیر ۱۸ سال تمام را آموزش داده یا تبلیغ یا تحریک یا تهدید یا تشویق یا دعوت نموده یا فریب دهد یا طریق ارتکاب یا استعمال آنها را تسهیل نماید یا آموزش دهد .

تبصره ۱: تولید یا ذخیره سازی یا تهیه محتویات غیر واقعی چنانچه به قصد ارایه یا انتشار یا قرار دادن در دسترس دیگران نباشد از شمول این ماده مستثنی است .

تبصره ۲: مفاد دو ماده فوق شامل آن دسته از محتویاتی که برای استفاده متعارف علمی یا هر مصلحت عقلایی دیگر ارایه می‌گردد، نخواهد بود.

امروزه حمایت از کودکان در برابر خطرات دنیای جدید که قسمت عمدهٔ آن در فضای سایبر تجلی یافته است، برای کلیه کشورها یک امر بدیهی شده است. در رأس این حمایتها، جرم‌انگاری هرزه‌نگاری کودکان است که بر اساس پروتکل اختیاری کنوانسیون حقوق کودک، پورنوگرافی یا هرزه‌نگاری کودکان به عنوان هر نوع شبیه‌سازی به فعالیت صریح جنسی یا نمایش اعضای جنسی کودک تعریف شده است. هرزه‌نگاری کودک می‌تواند به اشکال مختلف وجود داشته باشد. پورنوگرافی بصری کودک تشویق شده به فعالیت جنسی صریح، واقعی یا شبیه‌سازی یا نمایش وقیحانه اندام جنسی است. پورنوگرافی سمعی کودک استفاده از هر واسط صوتی استفاده کننده از صدای کودک، واقعی یا شبیه‌سازی، به قصد انگیزش جنسی کاربر است. پورنوگرافی کودک می‌تواند متن ساده‌ای باشد که به تشریح اعمال جنسی می‌پردازد یا به قصد انگیزش جنسی تهیه شده باشد.[۷] کنوانسیون جرایم محیط سایبر بوداپست مصوب ۲۳ سپتامبر ۲۰۰۱ در ماده ۹، مقررات مفصلی به جرایم مرتبط با هرزه‌نگاری کودکان اختصاص داده است که در این ماده تولید به قصد انتشار، ارایه یا در دسترس قرار دادن هرزه‌نگاری کودکان، پخش یا

۷- محمدحسن دزیانی، حمایت آن‌لاین از کوکان، خبرنامه انفوماتیک، سال هفدهم، آبان ۱۳۸۱ ، ص ۳۳

انتشار آنها و تهیه یا در اختیار داشتن هرزه‌نگاری اطفال را جرم تلقی کرده است و در بند ۲ این ماده هرزه‌نگاری محدود به تصاویر مستهجن شده است و برای کشورها سن ۱۸ سال جهت حمایت در برابر هرزه‌نگاری پیشنهاد شده و حداقل سن مورد حمایت به جای ۱۸ سال را ۱۶ سال قرار داده است. اما قبل از مقرره فوق در قالب کنوانسیون بوداپست، اکثر کشورها درصدد جرم انگاری پورنوگرافی اطفال برآمده بودند. کشورهایی مثل فرانسه و آلمان در قوانین جزایی خود در کنار مواد دیگر از اطفال نیز حمایت کرده‌اند. ایالت‌های آمریکا مقررات متنوعی در این زمینه دارند. حمایت از اطفال در اینترنت از سال ۱۹۹۶ و در زمان بیل کلینتون رییس‌جمهور آمریکا در این کشور آغاز شد. در قانون صلاحیت ارتباطات ۱۹۹۶ هرگونه اطلاع‌رسانی مستهجن و غیر اخلاقی برای نوجوانان کمتر از ۱۸ سال منع شده است. در سال ۱۹۹۸ قانون حمایت خصوصی اطفال بر خط[8] تصویب شد و پس از دو سال قانون حمایت از اطفال بر خط با جزئیات و حمایت‌های بیشتری تصویب شد.در انگلستان قانون حمایت از اطفال مصوب ۱۹۷۸ اصلاحی به وسیله قانون عدالت جزایی مصوب ۱۹۸۸ و قانون عدالت کیفری و نظم عمومی ۱۹۹۴ و قانون سوء استفاده از رایانه مصوب ۱۹۹۰ در زمینه حمایت از اطفال در محیط سایبر مقرراتی پیش‌بینی کرده‌اند.

در کشور ما حمایت از اطفال در محیط سایبر سابقهٔ تقنینی ندارد اما در زمینه حمایت از اطفال در برابر تصاویر مستهجن و مبتذل سابقه تقنینی وجود دارد. تبصره ۳ ماده ۳ قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت‌های غیر مجاز فعالیت می‌نمایند مصوب ۱۳۷۲/۱۱/۲۳ مقرر می‌دارد: *استفاده از صغار برای نگهداری، نمایش، عرضه، فروش و تکثیر نوارهای غیر مجاز موضوع این قانون موجب اعمال حداکثر مجازات‌های مقرره برای عامل خواهد بود.*

ماده ۲ و ۳ قانون حمایت از کودکان و نوجوانان مصوب زمستان ۱۳۸۱ به‌طور ضمنی به حمایت از اطفال در برابر محتویات هرزه پرداخته است. به استناد ماده ۲ این قانون *هر نوع اذیت و آزار کودکان و نوجوانان که موجب شود به آنها صدمه جسمانی یا روانی و اخلاقی وارد شود و سلامت جسم یا روان آنان را به مخاطره اندازد ممنوع است.* وفق ماده ۳ *هر گونه خرید، فروش، بهره‌کشی و به کارگیری کودکان به منظور ارتکاب اعمال خلاف از قبیل قاچاق ممنوع و مرتکب حسب مورد علاوه بر جبران خسارت وارده به ارتکاب اعمال خلاف از قبیل قاچاق ممنوع و مرتکب حسب مورد علاوه بر جبران خسارت وارده به شش ماه تا یکسال زندان و یا به جزای نقدی از ده میلیون ریال تا بیست میلیون ریال محکوم خواهد شد.*

این مقررات وقتی نوبت به فضای مجازی رایانه و اینترنت می‌رسد ناکافی به نظر می‌آید و لازم است که قانونگذار در این فضا بیش از بیش به وضعیت و موقعیت کوکی توجه نماید؛ زیرا شخصیت انسان در دوران کودکی و نوجوانی شکل می‌گیرد و در این دوران حساس که غریزه جنسی متلاطم‌ترین غریزه انسان است به راحتی و به هر شکلی قابل انحراف است و ممکن است صدمات جبران‌ناپذیری به فرد و جامعه وارد سازد. جرایم و انحرافات جنسی بیشترین قابلیت برای مزمن ساختن بزه‌کاری است. اصولاً بزه‌کاران مزمن که از همان دوران کودکی به کرات با ارتکاب جرم خو گرفته‌اند و نتوانسته‌اند این تکرار عادت را ترک کنند به نوعی با جرایم و انحراف جنسی دست به گریبان بوده‌اند. به همین دلیل پیشگیری زودرس در این زمینه بسیار لازم و ضروری است که نمونه برجسته آن کوتاه کردن دست استثمارگران جنسی و مرتکبین این جرایم از کودکان است. دنیای کودکان باید پاک و سالم و جهت‌یافته باشد تا سعادت آینده آنها و جامعه تأمین گردد. دنیای اینترنت یا فضای سایبر ظاهراً در این جا تیشه به ریشه شخصیت کودکان و اخلاق آنها می‌زند یا حداقل به‌طور جدی خود را آمادهٔ این کار ساخته است. حمایت

8- Children online private protection Act1998

از اطفال حمایت از آینده جامعه است و حمایت از آینده جامعه حمایت از بشریت و اخلاق است. به همین دلیل حمایت کیفری از اطفال مخصوصاً در دنیای سایبر و اینترنت بر تمام کشورها فرض شده است و در راستای حمایت کیفری همه جانبه از اطفال در کشورمان ماده ۱۶ لایحه پیش‌بینی شده است که ذیلاً به ارکان و اجزای این مقرره اشاره می‌شود:

۱ـ وسیله ارتکاب جرم: وسیله ارتکاب عمل مجرمانه صرفاً سیستم رایانه‌ای یا مخابراتی است و شامل محیط واقعی و خارجی نمی‌شود و بنابراین این جرم، زمانی که در محیط سایبر ارتکاب یافته باشد. قابل کیفر است. محتویاتی که به صورت مستهجن و یا مبتنی بر تبلیغ یا تحریک یا تشویق برای دستیابی به آنها هستند تنها در محیط سایبر قابل دیدن یا شنیدن هستند و الا در محیط خارج اگر عکس مستهجنی انتشار یابد یا فیلم مربوط به پورنوی اطفال در محیط بیرون ارایه گردد، مشمول این ماده نخواهد بود.

۲ـ بزه‌دیده جرم: بزه‌دیده جرایم موضوع این ماده فرد زیر ۱۸ سال تمام شمسی است؛ یعنی به محض اینکه وارد سن ۱۹ سالگی شدند، از شمول این حمایت خارج می‌شوند و این تفاوت از ۱۸ سال به ۱۹ سال صرفاً به لحاظ قراردادی و اعتباری قابل توجیه است؛ چه هر سنی که مقرر شود با سن بلا واسطه بعد از خود همین مشکل را خواهد داشت. اما حالتی که سن فرد برای مرجع رسیدگی کننده مشخص نباشد یا در محیط سایبر درج نشده باشد، در صورتی که ظاهراً آن شخص زیر ۱۸ سال تمام داشته باشد: مشمول این ماده می‌شود. این امر را می‌توان از ظاهر فرد یا سایت مورد نظر یا با عبارات و اصطلاحاتی، ویژه اطفال و نوجوانان فهمید که در این جا این ظاهریت یا شباهت فرد به افراد زیر ۱۸ سال باید از اشخاص بیمار یا استثنایی تفکیک شود و مرجع رسیدگی‌کننده باید به قدر متیقن عمل کند تا برحسب حدس و گمان کسی را دچار دام کیفر نسازد.

۳ـ رفتار فیزیکی جرم: رفتار فیزیکی جرم موضوع این ماده که نسبت به افراد زیر ۱۸ سال تمام صورت می‌پذیرد در قالب سه بند آمده است:

۳-۱-بند الف: تولید کردن یا ارایه نمودن یا انتشار دادن یا ذخیره‌سازی یا تهیه کردن یا در دسترس دیگران قرار دادن محتویات هرزه مربوط به اشخاص زیر ۱۸ سال یا ظاهراً زیر ۱۸ سال

تولید کردن: به معنای فرایند ایجاد یا ساختن تصویر یا صوت یا فیلم مربوط به نمایش اندام جنسی یا نمایش آمیزش یا عمل جنسی صریح از اشخاص زیر ۱۸ سال یا ظاهراً زیر ۱۸ سال است. تولید ممکن است پیچیده باشد و همراه با مجموعه‌ای از کارگردان، بازیگر، فیلمبردار و ... باشد و یا اینکه ساده باشد، به نحوی که ساختن یک تصویر یا صوت واقعی را دربرگیرد. تولید محتویات هرزه مربوط به اشخاص زیر ۱۸ سال اگر در محیط بیرون صورت بگیرد و سپس در اینترنت منتشر یا ارایه شود طبق این ماده جرم نیست؛ زیرا در فضای سایبر تحقق نیافته است؛ به عبارت دیگر سیستم رایانه‌ای یا مخابرات ارتکاب نیافته است. تولید محتویات غیر واقعی مثل نقاشی، تصاویر مصنوعی، طرح، انیمیشن، کارتون و ... که به صورت محتویات مستهجن باشند اگر با قصد ارایه یا انتشار یا در دسترس قرار دادن نباشد، جرم نیست و این قصد که تولید کننده محتویات غیر واقعی (نه محتویات واقعی از اشخاص واقعی که در هر صورت تولید صرف آنها جرم تلقی می‌شود)، این محتویات را در راستای ارایه یا انتشار یا در دسترس قرار دادن، تولید کرده، باید احراز شود که این امر از طریق قراینی همچون سابقه تولید کننده، میزان تولید، کیفیت تولید، سابقه روانی تولید کننده و وضعیت روحی فعلی او و ... حاصل می‌شود.

ارایه: ارایه مفهوم عامی است که شامل انتشار، عرضه، پخش، به نمایش گذاردن، نشان دادن و .... می‌شود که صرف ارایه کردن محتویات هرزه به اطفال برای اعمال کیفر این ماده کفایت می‌کند.

انتشار: انتشار یا پخش کردن در حد وسیع در زیر مجموعه "ارایه" قرار می‌گیرد و صرفاً در راستای تأکید آورده شده است.
در دسترس قرار دادن: این فعل نیز عام بوده و شامل رفتارهایی مثل خرید و فروش، هبه، عاریه، ودیعه، کرایه دادن، انتشار و ... است. به هر صورت مرتکب اگر به هر شکل محتویات هرزه را در اختیار یا در دسترس اشخاص زیر ۱۸ سال یا غیر آن قرار دهد، مجرم است.

انتشار، ارایه و در دسترس دیگران قرار دادن چه در محتویات واقعی و چه در محتویات غیر واقعی، احتیاجی به سوء نیت خاص ندارد و فرق نمی‌کند که این محتویات مربوط به اشخاص زیر ۱۸ سال یا ظاهراً زیر ۱۸ سال نسبت به اطفال انتشار یا ارایه یابند یا نسبت به اشخاص بیشتر از ۱۸ سال.

ذخیره‌سازی: به معنای انباشتن یا ذخیره کردن محتویات هرزه مربوط به اشخاص زیر ۱۸ سال یا ظاهراً زیر ۱۸سال در سیستم رایانه‌ای است و مکان ذخیره‌سازی ممکن است حافظه رایانه باشد یا سایت‌های اینترنت و یا حاملهای داده از قبیل سی‌دی یا دیسکت. ذخیره‌سازی محتویات هرزه از اشخاص زیر ۱۸ سال اگر واقعی باشند در هر صورت جرم است اما چنانچه ذخیره‌سازی از محتویات هرزه غیر واقعی از اشخاص زیر ۱۸ سال که به صورت تصاویر غیر واقعی، نقاشی، انیمیشن و ... باشند، اگر با قصد ارایه یا انتشار قرار دادن در دسترس دیگران نباشد، جرم نیست. (به استناد تبصره ۲ همین ماده)

تهیه: تهیه به معنای تدارک و به دست آوردن محتویات هرزه اطفال زیر ۱۸ سال یا ظاهراً زیر ۱۸ سال است. طریق تهیه به هر شکلی ممکن است. ممکن است به صورت هبه دریافت کرده باشد یا در اثر یک اتفاق با این محتویات برخورد و آنها را از طریق سیستم رایانه تهیه کرده باشد. تهیه محتویات غیر واقعی از اشخاص زیر ۱۸ سال اگر با قصد ارایه یا انتشار یا قرار دادن در دسترس دیگران نباشد، جرم نیست.

قابل ذکر است که ذخیره‌سازی، تهیه و تولید به عنوان بخشی از رفتارهای فیزیکی موضوع بند الف این ماده فقط ناظر به هرزه نگاری اطفال است. ارایه، انتشار و در دسترس دیگران قرار دادن نیز صرفاً ناظر به محتویات هرزه اطفال است و لیکن ارایه یا انتشار یا در دسترس دیگران قرار دادن ممکن است هم نسبت به اطفال زیر ۱۸ سال صورت گیرد و هم بزرگسال که قاضی می‌تواند حسب مورد ارایه یا انتشار پورنوی اطفال به اطفال را به عنوان کیفیات مشدده مجازات تلقی کند. با این وصف با توجه به ماده قبلی و این ماده انتشار یا ارایه یا در دسترس قرار دادن به صورت زیر تقسیم بندی می‌شود:

۱ـ انتشار یا معامله محتویات هرزه بزرگسالان به بزرگسالان	←	حبس ۳ ماه و یک روز تا یکسال یا جزای نقدی یا هر دو آنها
۲ـ ارایه یا در دسترس قرار دادن محتویات هرزه بزرگسالان به بزرگسالان	←	جرم نیست.
۳ـ انتشار یا در دسترس قرار دادن محتویات هرزه بزرگسالان به اطفال	←	حداکثر مجازات یعنی یکسال حبس یا جزای نقدی ده میلیون ریال یا حداکثر هر دو
۴ـ ارایه یا انتشار یا در دسترس قرار دادن محتویات هرزه کودکان به بزرگسالان	←	حبس از یک تا ۳ سال یا جزای نقدی یا هر دوی آنها
۵ـ ارایه یا انتشار یا در دسترس قرار دادن محتویات هرزه کودکان به کودکان	←	مجازات فوق که در این جا قاضی با توجه به اینکه مخاطب جرم، طفل است، می‌تواند مجازات را به مراتب تشدید کند.

۳-۲- بند ب: تبلیغ یا تحریک یا تشویق یا دعوت یا فریب یا تهدید به دستیابی به محتویات هرزه موضوع بند الف این ماده یا محتویات موضوع ماده مربوط به بزرگسالان (ماده قبل) یا تسهیل یا آموزش طریق دستیابی به آنها. رفتار فیزیکی موضوع این بند شامل مصادیق رفتاری معاونت در جرم است که بخش اعظم آن در ماده ۴۳ قانون مجازات اسلامی آمده است و لزومی به توضیح درباره آنها نیست. در این جا به نوعی معاونت در حکم جرم مستقل است و دیگر بحث از معاونت نیست بلکه سخن از مباشرت است. تبلیغ یا تحریک کننده در این جا مباشر جرم است و رفتارهای موضوع این بند باید نسبت به اشخاص زیر ۱۸ سال تمام صورت بگیرد. در این جا قید «ظاهراً زیر ۱۸ سال» آورده نشده است ؛ چون محتویات، مربوط به تصویر یا صدا یا فیلم نیست و بنابراین قاضی باید احراز نماید که رفتارهای مجرمانه موضوع این بند نسبت به شخص زیر ۱۸ سال تمام صورت گرفته باشد. محتویات هرزه اعم است از اینکه مربوط به اشخاص زیر ۱۸ سال یا ظاهراً زیر ۱۸ سال یا مربوط به اشخاص بالای ۱۸ سال باشد. بنابراین رفتارهای موضوع این بند ممکن است نسبت به محتویات هرزه بزرگسالان (موضوع ماده قبل) صورت بگیرد. نتیجتاً رفتارهای مجرمانه موضوع بند ب عبارتند از:

۱ـ تبلیغ یا تحریک یا تشویق یا دعوت (چه به صورت عمومی باشد و چه خصوصی) یا فریب یا تهدید اشخاص زیر ۱۸ سال تمام به دستیابی به محتویات هرزه کودکان یا بزرگسالان

۲ـ تسهیل یا آموزش طریق دستیابی اشخاص زیر ۱۸ سال تمام به محتویات هرزه کودکان یا بزرگسالان

۳-۳- بند ج: تبلیغ یا تحریک یا تشویق یا دعوت یا فریب یا تهدید اشخاص زیر ۱۸ سال تمام به ارتکاب جرایم و انحرافات جنسی یا سایر جرایم یا خودکشی یا استعمال مواد روانگردان یا تسهیل یا آموزش طریق ارتکاب یا استعمال آنها.

بنابراین رفتار فیزیکی جرایم موضوع بند ج را می‌توان به این صورت احصاء کرد:

الف) تبلیغ یا تحریک یا تشویق یا دعوت یا فریب یا تهدید به ارتکاب جرایم و انحرافات جنسی یا سایر جرایم یا خودکشی: رفتارهای مجرمانه فوق به غیر از «دعوت» همگی از مصادیق معاونت در جرم موضوع ماده ۴۳ قانون مجازات اسلامی هستند که در این جا به عنوان جرم مستقل پیش‌بینی شده‌اند. تمام این رفتارهای مجرمانه باید نسبت به اشخاص زیر ۱۸ سال تمام صورت بگیرد تا مستوجب کیفر گردد و در این جا قاضی باید لزوماً سن مقرر را برای شخص بزه‌دیده را احراز نماید وگرنه در مقام تردید و یا در جائیکه ظاهراً ۱۸ سال تمام است، اعمال کیفر، وجهه قانونی ندارد. تمام رفتارهای مجرمانه فوق باید صراحتاً و مشخصاً نسبت به اشخاص زیر ۱۸ سال صورت بپذیرد چه به عموم اشخاص زیر ۱۸سال و چه به صورت خصوصی. پس تحریک یا تشویق به ارتکاب جرم در محیط سایبر به صورت عام جرم تلقی نمی‌شود.

در این جا علاوه بر تبلیغ یا تحریک یا تشویق یا دعوت یا فریب یا تهدید به ارتکاب جرایم (که جرایم جنسی به لحاظ تأکید و اهمیت ذکر شده است) تحریک یا تشویق یا دعوت به ارتکاب برخی از انحرافات نیز در نظر گرفته شده‌که دو مورد است:

الف-۱- انحرافات جنسی: انحرافات جنسی علاوه بر اینکه شامل اکثر جرایم جنسی می‌شود، شامل برخی رفتارهای دیگر نیز می‌گردد که عنوان مجرمانه ندارند مثل ارضای جنسی با حیوانات، ارضای جنسی با اشیاء، خود ارضایی و ... که اثر مخرب این انحرافات بر روی اشخاص زیر ۱۸ سال در برخی مواقع از اثر مقاربت بین دختر و پسر بیشتر است. از این رو لازم است تا اشخاص زیر ۱۸ سال در برابر این انحرافات مصونیت یابند و به همین لحاظ تبلیغ یا تحریک یا تشویق یا دعوت یا فریب یا

تهدید به ارتکاب انحرافات جنسی که برای جامعه‌شناسان و جرم‌شناسان شناخته شده، جرم تلقی شده است. قاضی برای تعیین انحرافات جنسی باید به عرف پزشکان، جرم‌شناسان و روان‌شناسان مراجعه کند.

الف ـ۲ـ خودکشی: خودکشی در کشور ما جرم نیست اما انحراف است. در خیلی از کشورها معاونت در خودکشی جرم تلقی شده است و لازمه آن وقوع خودکشی است، اما در مقرره مورد بحث وقوع خودکشی از سوی شخص زیر ۱۸ سال تمام لازم نیست کما اینکه در مورد انحرافات جنسی یا سایر جرایم نیز ارتکاب آنها توسط شخص زیر ۱۸ سال تمام شرط تحقق جرم موضوع بند ج، نخواهد بود.

ب) استعمال مواد روانگردان: مواد یا داروهای روانگردان هرگونه ماده طبیعی یا ترکیبی هستند که حالت روانی و جسمی را دگرگون می‌سازد. این مواد یا داروها در کنوانسیون داروهای روانگردان مصوب ۱۹۷۱ احصا شده‌اند که در کنوانسیون سازمان ملل متحد برای مبارزه با قاچاق مواد مخدر و داورهای روانگردان مصوب ۲۰ دسامبر ۱۹۸۸ و در قالب ماده ۳ این کنوانسیون جرم انگاری شده‌اند. ایران با تصویب مجلس شورای اسلامی مصوب ۱۳۷۰/۹/۳ و تأیید شورای نگهبان مصوب ۱۳۷۰/۹/۱۷ به این کنوانسیون ملحق شده است. قسمت (و) از بند ۵ مادهٔ ۳ این کنوانسیون اغوا یا استفاده از کودکان را از کیفیات مشددهٔ واقعی دانسته است. بند (ج) مادهٔ ۱۶مورد بحث، یکی از طرق پیوستن به این کنوانسیون مهم است که قاضی برای تعیین مواد روانگردان باید به کنوانسیون مواد روانگردان ۱۹۷۱ و کنوانسیون ۱۹۸۸ مراجعه کند.

ج) تسهیل یا آموزش ارتکاب جرایم یا انحرافات جنسی یا خودکشی یا تسهیل یا آموزش استعمال مواد روانگردان:

تسهیل یا آموزش همانند سایر رفتارهای مندرج در این بند فقط از طریق سیستم رایانه‌ای و اینترنت قابل تحقق است و الا خلاء قانونی در قوانین دیگر را نمی‌توان در این جا جبران کرد تا از این طریق این مورد را به محیط واقعی و بیرونی نیز تسری داد.

تمامی جرایم موضوع ماده مورد بحث در هر سه بند مطلق هستند و لزومی به حصول نتیجه مجرمانه نیست.

۴ـ رکن روانی :جرایم موضوع مورد بحث تماماً عمدی هستند و صرف عمد مرتکب در ارتکاب رفتارهای قبل‌الذکر کفایت می‌کند با این دو شرط که اولاً مرتکب باید علم داشته باشد که بزه دیده او شخص یا اشخاص زیر ۱۸ سال تمام هستند و او نیز با این علم رفتارهای مجرمانه قبل‌الذکر را انجام دهد مگر در ارایه یا انتشار یا در دسترس قرار دادن محتویات هرزه مربوط به اشخاص زیر ۱۸ سال تمام یا ظاهراً زیر ۱۸ سال که فرقی نمی‌کند به شخص زیر ۱۸ سال ارایه یا انتشار یابند یا به اشخاص بیش از ۱۸ سال. ثانیاً رفتارهای مجرمانه مورد بحث دارای سوءنیت خاص نیستند مگر در تولید یا ذخیره‌سازی یا تهیه محتویات غیر واقعی که باید قصد ارایه یا انتشار یا قرار دادن در دسترس دیگران احراز شود. (تبصره این ماده)

براساس تبصره ۲ ماده ۱۶، مفاد دو ماده فوق شامل آن دسته از محتویاتی که برای استفاده متعارف علمی یا هر مصلحت عقلایی دیگر ارایه می‌گردد، نخواهد بود. چون در این جا سوءنیت یا به عبارتی کەروانی وجود ندارد و محتویات مورد بحث، جنبه علمی یا آموزش مجاز دارند.

۵ـ مجازات: مجازات مقرر در ماده مورد بحث بر دو قسم است:

الف) حبس از یک تا ۳ سال یا جزای نقدی از ده میلیون تا سی میلیون ریال یا هر دو مجازات برای تولید یا ارایه یا انتشار یا ذخیره‌سازی یا در دسترس قرار دادن محتویات هرزه اشخاص زیر ۱۸ سال.

کیفر فوق با توجه به مقررات قانون مجازات اسلامی و بویژه ماده ۶۴۰ و با توجه به اینکه این رفتارهای مجرمانه نسبت به اطفال بسیار مخرب است، تقریباً سنگین می‌باشد و با سایر کیفرها از لحاظ میزان و شدت متفاوت است. جزای نقدی و

حبس دارای حداقل و حداکثر است تا مرجع رسیدگی کننده بتواند با توجه به کیفیت و کمیت ارتکاب جرم و سابقه وی و شرایط و تعداد بزه‌دیده، مجازات متناسب را تشخیص دهد.

ب) حبس از سه ماه و یک روز تا یکسال یا جزای نقدی از دو میلیون و پانصد هزار تا ده میلیون ریال یا هر دو مجازات برای تبلیغ یا تحریک یا تشویق یا دعوت یا فریب یا تهدید اشخاص زیر ۱۸ سال تمام به دستیابی به محتویات هرزه بزرگسالان یا اطفال یا ارتکاب جرایم و انحرافات جنسی یا سایر جرایم یا خودکشی یا استعمال مواد روانگردان و همچنین تسهیل یا آموزش طریق ارتکاب جرایم یا انحرافات جنسی یا استعمال مواد روانگردان یا طریق دستیابی به محتویات هرزه بزرگسالان یا کودکان.

کیفر اختیاری و خفیف این دو بند (ب و ج) نسبت به بند الف به این دلیل است که اولاً رفتارهای مجرمانه در این جا اکثراً رفتارهای معنوی و از مصادیق ذاتی معاونت در جرم است که عنوان مستقل یافته‌اند. ثانیاً در این جا لزومی به وقوع نتیجه از عملکرد مرتکب نیست. بنابراین صرف تبلیغ، تحریک، تشویق و .... با سوءنیت کفایت می‌کند.

قابل ذکر است جرایم موضوع دو ماده مربوط به محتویات هرزه اطفال و بزرگسالان در زمره جرایم غیر قابل گذشت است و شروع به جرم آنها , جرم محسوب **نمی‌شود**.

۵-۳- هرزه نگاری و تحریف نگاری شخصیت

ماده ۱۷ مقرر می دارد: « **هر کس از طریق سیستم رایانه ای یا مخابراتی فیلم یا تصویر یا صوت دیگری را تغییر دهد یا تحریف نماید و منتشر سازد یا با علم به تحریف یا تغییر، انتشار دهد، به نحوی که منجر به هتک حرمت یا ضرر غیر گردد به حبس از نود و یک روز تا شش ماه یا پرداخت جزای نقدی از دو میلیون و پانصد هزار تا ده میلیون ریال محکوم خواهد شد».**

تبصره: ارتکاب جرم موضوع این ماده نسبت به مقام رهبری یا روسای قوای سه گانه مستوجب حداکثر حبس یا جزای نقدی مقرر در این ماده خواهد بود.

جرم موضوع ماده فوق ناظر به دو عنوان مجرمانه است که در هم ادغام شده است: *الف) هرزه‌نگاری هویت* :که شامل تحریف و تغییر فیلم، تصویر و صوت دیگری است که به صورت مستهجن یا مبتذل درآمده است. این تصاویر یا فیلم یا صوتهای مستهجن ممکن است واقعی باشند و از روی نسخه واقعی به این صورت درآمده باشند و همچنین ممکن است به صورت غیر واقعی باشند اما کاملاً شبیه به تصویر، فیلم یا صوت یک یا چند شخص معین باشد. *ب) تحریف‌نگاری هویت* : شامل تصاویر، فیلم و صوتی است که تحریف یا تغییر یافته که در نتیجه آن، هتک حرمت شخصی شده یا به دیگری ضرر وارد شود.

وضع ماده ۱۷ از آن جهت بوده است که محیط سایبر فضای مناسبی برای اهانت و هرزه‌نگاری شخصیت گشته است. در این فضا به راحتی می‌توان تصاویر یا فیلمها یا صوتهای اشخاص و به ویژه مسوولین مملکت را تغییر داد, به طوری که از یک سو به راحتی در دام عدالت گرفتار نشد و از سوی دیگر زشت‌ترین و زننده‌ترین تصاویر، فیلمها و صوتها را به دیگران منتسب ساخت. هر چند عموماً ناظرین این صحنه‌ها این محتویات را به صاحبان اصلی آنها منتسب نمی‌دانند اما موجب اهانت به اشخاص و مخصوصاً مسئولین مملکتی و تزلزل حرمت شخص می‌گردد. فضای سایبر در این زمینه به قدری مساعد است که

هم اکنون هر تصویری که در مخیله انسان می‌گنجد، می‌توان در آن یافت و این محیط افسارگسیخته قطعاً باید کنترل شود. ارکان وشرایط تشکیل دهنده جرم موضوع این ماده به شرح زیر است:

۱ـ موضوع مجرمانه: موضوع جرم در واقع هدف و سیبل جرم است. که جرم علیه آن واقع می‌شود. موضوع جرم در ماده ۱۷ فیلم، تصویر و صوت دیگری است. فیلم یا تصویر یا صوت دیگری ممکن است واقعی دیگری باشند و مرتکب آنها را تغییر دهد. همچنین فیلم یا تصویر یا صوت ممکن است غیر واقعی باشند و در اثر سیستم رایانه‌ای تولید شده باشند اما شباهت عرفی با فیلم یا تصویر یا صوت یک شخص معین دارد. تصاویر، فیلم‌ها یا اصوات واقعی ممکن است در فضای سایبر نباشند و مرتکب آنها را از محیط بیرون، وارد محیط سایبر کرده است و سپس مبادرت به تغییر و تحریف آنها نموده باشد. ضمناً اگر صوت یا تصویر یا فیلم با هم جمع شوند؛ یعنی صوت همراه با تصویر یا فیلم باشد، تغییر یا تحریف یکی از آنها برای تحقق موضوع مجرمانه این ماده با حصول سایر شرایط دیگر کفایت می‌کند.

۲ـ وسیله ارتکاب جرم: وسیله ارتکاب جرم، سیستم رایانه‌ای یا مخابراتی است. بنابراین تمام ارکان فیزیکی جرم موضوع این ماده باید در فضای مجازی اینترنت و مخابرات تحقق یابد. تغییر و تحریف‌نگاری هویت به نحویکه منجر به هتک حیثیت فرد دیگری شود، توسط سیستم رایانه‌ای که اینترنت بخشی از این سیستم است، به راحتی صورت می‌گیرد. در این سیستم نرم‌افزارهای بسیار متنوعی وجود دارد که با کمک آنها می‌توان هر تصویری را تغییر داد یا هر صوت و فیلم و تصویر را خلق کرد و از این حیث به راحتی می‌تواند وسیله سوء استفاده از حیثیت و آبروی دیگران گردد. اما اینکه سیستم مخابراتی چگونه می‌تواند وسیله ارتکاب جرم موضوع این ماده واقع شود باید گفت که می‌توان از طریق دستکاری در امواج الکترومغناطیسی یا بواسطه سیستم ارتباطی صوت دیگری را تقلید کرد یا تحریف کرد و یا اینکه با استفاده از همین سیستم، صوت تحریف شده را بر روی فیلم متحرک گذاشت.

۳ـ رفتار مادی جرم: جرم موضوع این ماده هم جرم مرکب است و هم جرم ساده جرم مرکب است از این حیث که اگر شخصی مبادرت به تحریف یا تغییر تصویر، صوت یا فیلم نماید تا زمانیکه تصویر، صوت و فیلم تغییر یا تحریف یافته را منتشر نسازد، مرتکب جرم موضوع ماده ۱۷ نشده است. بنابراین جرم تحریف‌نگاری هویت با توجه به عمل فیزیکی مرتکب یا مرکب است یا ساده.

الف) تحریف‌نگاری هویت به صورت مرکب: جرم مرکب جرمی است که فعل فیزیکی آن دو یا چند فعل متفاوت است که در این جا ابتدا تحریف یا تغییر است و سپس انتشار. تحریف عبارتست از منحرف ساختن اصل و اساس چیزی. بنابراین این اصل و اساس ممکن است در دسترس مرتکب نباشد و لیکن از تصویر یا صوت یا فیلمی که شناخته شده است، تصویر یا صوت یا فیلم دیگری را می‌سازد که منحرف و منصرف از اصل خود است و عرف نیز این شباهت را از یک سو و انحراف‌دهی را از سوی دیگر درک می‌کند. اما تغییر به مفهوم دگرگون ساختن یک چیز واقعی است و ناظر به ساختن یک چیز غیر واقعی نمی باشد. بنابراین اگر شخص یک تصویر، فیلم یا صوت واقعی دیگری را جزئاً دگرگون نماید در این جا این محتویات را تغییر داده است و اگر از اساس تصویر، فیلم یا صوت غیر واقعی ایجاد نماید که شبیه به تصویر، فیلم یا صوت واقعی دیگری است، محتویات را تحریف ساخته است. انتشار ناظر به توزیع و پخش چیزی در حد وسیع در میان مردم است که عرفاً به آن انتشار گفته می‌شود؛ مثل انتشار روزنامه. طبق قسمت اول ماده مورد بحث اگر شخصی مرتکب تحریف یا تغییر فیلم یا تصویر یا صوت دیگری شود در صورتی براساس ماده ۱۷ مجازات می‌شود که محتویات تغییر یا تحریف یافته را منتشر نماید.

ب ـ تحریف‌نگاری هویت به صورت ساده: صرف انتشار فیلم یا تصویر یا صوت تغییر یا تحریف یافته دیگری با علم به تغییر یا تحریف آنها جرم است، هر چند مرتکب خود محتویات مورد نظر را تغییر یا تحریف نداده باشد.

۴ـ نتیجه مجرمانه: جرم تحریف‌نگاری هویت یک جرم مقیّد به حصول نتیجه مجرمانه است که حصول یکی از نتایج مجرمانه زیر برای تحقق جرم کفایت می‌کند.

۴-۱ـ *هتک حرمت:* هتک حرمت در اینجا ناظر به قذف یا توهین یا افترا نیست و اگر تغییر یا تحریف متضمن نوعی قذف، توهین یا افترا گردد، بر اساس قانون مجازات اسلامی مجازات می‌شود. هتک حرمت بیشتر متکی بر یک مفهوم عرفی از آبروریزی، کسر شأن و اعتبار و شکستن حرمت دیگری است.

۴-۲- *ایراد ضرر:* ایراد ضرر بر اثر تحریف‌نگاری هویت اعم از مادی و معنوی است. ایراد ضرر مادی توسط قاضی یا کارشناس قابل تعیین است اما ایراد ضرر معنوی با توجه به شرایط و اوضاع و احوال ارتکاب جرم، موقعیت بزه‌دیده و نحوه انعکاس جرم در جامعه، به وسیله قاضی تشخیص داده می‌شود و تعیین آنها ممکن است به عهده کارشناس قرار گیرد.

۵ـ رکن روانی: جرم موضوع این ماده عمدی است و باید در فعل فیزیکی تغییر و تحریف، عمد وجود داشته باشد. در انتشار فیلم یا تصویر یا صوت تغییر یافته علم به تغییر یا تحریف یافتگی برای مرتکب شرط است و الا اگر مرتکب بدون علم به تغییر یافتگی فیلم یا تصویر یا صوت آنها را منتشر سازد، هرچند به صورت مستهجن باشند، براساس این ماده قابل کیفر نیست و حسب مورد ممکن است به مجازات مقرر دو ماده قبل مربوط به هرزه‌نگاری محکوم گردد.

۶ـ کیفیت مشدده مجازات: تحریف‌نگاری هویت اگر نسبت به مقام رهبری یا روسای قوای سه‌گانه صورت بگیرد، مرتکب به حداکثر مجازات مقرر در ماده محکوم می‌شود. بنابراین کیفیات مشدده ماده مورد نظر زمانی به طور اجباری بر مرتکب تحمیل می‌شود که جرم نسبت به مقام‌های کلیدی که شناخته شده هستند و امور مهم کشور براساس تصمیم‌گیری آنها جریان می‌یابد، ارتکاب یابد که این مقام‌ها عبارتند از: رهبر و رؤسای قوای سه گانه. ارتکاب جرم نسبت به اشخاص دیگر، خارج از تبصره ماده مورد نظر و طبعاً بیرون از کیفیات مشدده می‌باشد.

البته در مقام تفسیر مضیق قوانین جزایی بایدگفت این جرم باید نسبت به مقام آنها صورت بگیرد؛ یعنی تحریف یا تغییر صوت یا تصویر یا فیلم با توجه به سمت و مقام آنها صورت بگیرد نه نسبت به شخصیت خصوصی آنها. در غیر این صورت همانند افراد عادی مشمول ماده ۱۷ می‌شود؛ مثلاً شخصی ممکن است صدای رئیس‌جمهور را در جایی که در مقام رئیس جمهوری انجام وظیفه می‌کند، تحریف کند که در این جا مشمول کیفیات مشدده است اما اگر صدای رئیس‌جمهور را که با بستگان خصوصی یا با زنش صحبت می‌کند، تحریف کند، این مورد مشمول کیفیات مشدده نمی‌شود.

۷ـ جرم موضوع این ماده به استناد تبصره ماده ۱۹ قابل گذشت است مگر اینکه جرم نسبت به مقام رهبری یا روسای قوای سه گانه ارتکاب یابد. که در این جا جرم غیر قابل گذشت است.

۸ـ مجازات کیفر مقرر برای جرم موضوع این ماده به‌طور اختیاری یکی از دو کیفر زیر است:

۱ ـ حبس از ۹۱ روز تا شش ماه تا به بلحاظ سبکی جرم ارتکابی مشمول قانون مجازات‌های اجتماعی و تبدیلی شود.

۲ـ جزای نقدی از دو میلیون و پانصد هزار تا ده میلیون ریال

۵-۴- : انتشار یا در دسترس قرار دادن اسرار خصوصی

ماده ۱۸ مقرر می دارد: « **هر کس از طریق سیستم رایانه‌ای یا مخابراتی فیلم یا تصویر یا صوت یا اسرار خصوصی یا خانوادگی دیگری را بدون رضایت وی منتشر نماید یا در دسترس دیگران قرار دهد، به نحویکه منجر به ضرر غیر گردد یا عرفاً موجب هتک حیثیت وی شود به حبس از نود و یک روز تا شش ماه یا پرداخت جزای نقدی از دو میلیون و پانصد هزار تا ده میلیون ریال محکوم خواهد شد».**

جرم موضوع: این ماده را از یک جهت نمی‌توان در زیر مجموعه جرایم مرتبط با محتوا آورد؛ زیرا محتویات موضوع این ماده دارای صاحب مشخصی بوده و ازرشمند و قابل حمایت‌اند. اما از جهت دیگر محتویات فوق فقط برای صاحبان آنها دارای ارزش بوده و فاقد ارزش همگانی است. همچنین به لحاظ اینکه در این‌جا، محتوای قابل حمایت از طریق انتشار یا ارایه وسیله‌ای برای هتک حیثیت افراد می‌باشد، شباهتهایی از جهت آثار جرم با جرایم مرتبط با محتوا دارد که باعث شده است، جرم موضوع ماده ۱۸ را در ردیف جرایم مرتبط با محتوا ذکر کنیم. البته در مقام تعریف عام جرایم مرتبط با محتوا، جرم موضوع ماده مورد بحث، در ارتباط با محتویات خانوادگی و خصوصی افراد داخل در مصادیق این قسم از جرایم است.

توصیف مجرمانه ماده فوق انتشار یا در دسترس قرار دادن فیلم یا تصویر یا صوت یا اسرار خصوصی یا خانوادگی دیگری بدون رضایت است. این ماده درصدد حمایت از حریم خصوصی افراد است و در واقع توجیه جرم‌انگاری آن در راستای تأمین امنیت و آسایش خصوصی افراد است. انتشار اسرار یا تصاویر خصوصی افراد در برخی مواقع می‌تواند آثار زیانباری بـــر بزه‌دیده داشته باشد و حال آنکه در مقررات کلاسیک ایران در این زمینه جرم‌انگاری نشده است. در سال ۱۳۸۰ در پی انتشار فیلم جشن خصوصی دختران دانشجوی یکی از استانهای کشورمان، به یک یا دو نفر مبادرت به خودکشی کردند. در حالیکه نفس عمل انتشار دهنده در مقررات فعلی جرم نبود. اینترنت و رایانه و مخابرات بهترین وسیله برای انتشار یا در دسترس قرار دادن اسرار یا تصاویر خصوصی افراد است و همین امر به شدت حریم خصوصی افراد را تهدید می‌کند.

ارکان تشکیل دهنده جرم موضوع این ماده به شرح زیر است:

۱ـ موضوع مجرمانه: موضوع جرم در این ماده فیلم یا تصویر یا صوت یا اسرار خصوصی یا خانوادگی است. منظور از فیلم، تصاویر متحرک واقعی افراد است که عمدتاً شامل نشستها، جشنها و مسافرت‌های خصوصی و از این قبیل می گردد. تصویر شامل عکس، نقاشی یا هر طرحی می گردد که جنبه محرمانه و خصوصی داشته باشد. عکس و همچنین نقاشی یا هر طرح دیگر وقتی شامل این ماده می‌شود که اولا ارتباط مستقیم با حریم خصوصی افراد داشته باشد و کلا محرمانه و خصوصی تلقی شود و ثانیاً موضوع حقوق و مقررات دیگر همچون کپی رایت نگردد. بنابراین انتشار یا دردسترس قرار دادن محتوایی که در زمره حق تألیف، حق ترجمه، حق اختراع و از این قبیل حقوق باشد، بر اساس مقررات جزایی مربوطه رفتار خواهدشد.

صوت شامل صدای واقعی است و اسرار خصوصی یا خانوادگی شامل هر چیزی می‌شود که دسترسی دیگری به آنها عمدتاً با عدم رضایت صاحب آن مواجه می‌گردد و عرفاً جنبه سر داشته باشند. اسرار خصوصی لزوماً شامل اسرار خانوادگی نمی‌شود؛ مانند نشستها یا جشنهای خصوصی چند دوست یا هم‌کلاسی در یک مکان مشخص.

موضوع جرم مورد نظر در هر صورت باید واقعی باشد؛ یعنی نسبت به آن شبیه‌سازی یا دخل و تصرف و یا تغییر صورت نگرفته باشد. در غیر این صورت حسب مورد جعل، تخریب یا تحریف‌نگاری یا هرزه نگاری هویت خواهد بود.

۲ـ وسیله ارتکاب جرم: وسیله ارتکاب عمل مجرمانه در این ماده سیستم رایانه‌ای یا مخابراتی است و به عبارت دیگر جرم و مجازات موضوع ماده فوق‌الذکر فقط در فضای سایبر یا فضای مجازی اینترنت و مخابرات قابل تحقق است. هر چند چنین جرمی توسط وسایل دیگر هم قابل ارتکاب است و از سویی نیز در مقررات کیفری دیگر در این زمینه ضمانت اجرای کیفری پیش‌بینی نشده است، به تبع جرم‌انگاری در فضای سایبر بر مراجع تقنینی است که اولاً محدوده حریم خصوصی افراد را مشخص نمایند و ثانیاً تجاوزات به این حریم را جرم‌انگاری نمایند.

۳ـ رفتار مادی جرم: فعل فیزیکی جرم موضوع ماده ۱۸، منتشر ساختن یا در دسترس دیگران قرار دادن فیلم یا تصویر یا صوت یا اسرار خصوصی یا خانوادگی است. انتشار، ناظر به توزیع محتویات ذکر شده در میان چندین نفر است که عرفاً از آن به انتشار تلقی شود. در دسترس دیگران قرار دادن به معنای ارایه محتویات ذکر شده به هر نحو به دیگری است اعم از خرید و فروش، به امانت سپردن، بخشیدن و ....که در اثر ارایه این تصاویر، عکسها، فیلمها و کلاً اسرار خصوصی و خانوادگی به دیگری ممکن است مشکلات و اختلافات بسیار زیادی در روابط خصوصی و خانوادگی افراد پیش آید.

۴ـ شرط عدم رضایت: عدم رضایت صاحب فیلم یا تصویر یا صوت یا اسرار خصوصی یا خانوادگی در انتشار یا در دسترس قرار دادن آنها شرط لازم تحقق جرم موضوع ماده ۱۸ است. به لحاظ تفسیر مضیق مقررات کیفری باید گفت که عدم رضایت درونی یا سکوت صاحب محتویات فوق کفایت نمی‌کند و بلکه باید عدم رضایت خود در انتشار یا در دسترس قرار دادن اسرار خصوصی و خانوادگی یا تصاویر، فیلم یا صوتش را اعلام بکند. عدم رضایت ممکن است قبل از وقوع جرم باشد و ممکن است پس از اطلاع از انتشار یا در دسترس قرار دادن، این عدم رضایت هویدا گردد که قرینه برجسته آن شکایت صاحب محتویات است. اما اگر قبل از انتشار یا در دسترس قرار دادن، صاحب محتویات دارای رضایت بوده و این رضایت کشف شود، نمی‌تواند پس از انتشار یا ارایه ادعای وقوع جرم موضوع ماده ۱۸ را بنماید. رضایت حالت درونی شخص نسبت به وضعیت خود است و بنابراین در قالب یک حق متصور نیست تا قابل انتقال یا تورث باشد.

۵ـ نتیجه مجرمانه: جرم انتشار یا در دسترس دیگری قرار دادن محتویات خصوصی دیگری، در زمره جرایم مقید به حصول نتیجه است که حصول یکی از نتایج زیر برای تحقق جرم مورد نظر کفایت می‌کند:

۵-۱- *ایراد ضرر به غیر*: ضرر وارده در اثر انتشار یا در دسترس قرار دادن محتویات خصوصی دیگری ممکن است مادی باشد و یا معنوی که در هر صورت این ضرر تحقق می‌یابد. نتیجه مجرمانه جرم موضوع ماده ۱۸بیشتر ضرر معنوی است و این ضرر معنوی براساس قانون اساسی جمهوری اسلامی ایران (اصل ۱۷۱ ق . اساسی) قابل مطالبه است.

۵-۲- *هتک حیثیت عرفی*:انتشار یا ارایه تصاویر، فیلم یا اسرار خصوصی و خانوادگی از منظر عرف ممکن است موجب هتک حیثیت شود. منظور از هتک حیثیت، افتراء، قذف یا توهین نیست و بلکه منظور آبروریزی یا حیثیت رفتگی است که عرف گواه بر آن است و الا اگر انتشار یا ارایه محتویات موضوع ماده ۱۸ مشمول افتراء، قذف یا توهین باشد، براساس قانون مجازات اسلامی قابل محاکمه هستند نه این ماده و این ماده صرفاً شامل مواردی می‌شود که انتشار یا ارایه محتویات فوق‌الذکر موجب آبروریزی یا کسر شأن و حیثیت فرد می‌شود.

۶ـ به استناد تبصره ماده ۱۹، جرم موضوع ماده ۱۸ در زمرهٔ جرایم قابل گذشت است که جز با شکایت خصوصی تعقیب نمی‌شود و با گذشت وی تعقیب موقوف خواهد شد.

۷ ـ مجازات ضمانت اجرای مقرر برای این جرم یکی از دو کیفر زیر است:

الف ـ حبس از ۹۱ روز تا شش ماه تا به لحاظ خفیف بودن جرم مشمول مجازات‌های مناسب اجتماعی و تبدیلی شود. ب ـ جزای نقدی از دو میلیون و پانصد هزار تا ده میلیون ریال

۵-۵- نشر اکاذیب

ماده ۱۹ مقرر می دارد: **« هر کس از طریق سیستم رایانه ای یا مخابراتی اکاذیبی را منتشر نماید یا در دسترس دیگران قرار دهد یا اعمالی را بر خلاف حقیقت راساً یا به عنوان نقل قول به شخص حقیقی یا حقوقی یا مقامات رسمی نسبت دهد به نحویکه موجب تشویش اذهان عمومی یا مقامات رسمی یا ضرر غیر شود، علاوه بر اعاده حیثیت به حبس از سه ماه و یک روز تا شش ماه یا پرداخت جزای نقدی از دو میلیون و پانصد هزار تا ده میلیون ریال محکوم خواهد شد».**

تبصره: جرایم موضوع مواد ۱۷ (به استثنای تبصره این ماده) ۱۸ و ۱۹ (به استثنای نشر یا در دسترس قرار دادن اکاذیب یا نسبت دادن اعمال خلاف حقیقت که موجب تشویق اذهان عمومی یا مقامات رسمی گردد) جز با شکایت شاکی خصوصی تعقیب نمی‌شود و با گذشت وی تعقیب موقوف خواهد شد.

این ماده با برخی تغییرات اندک تکرار ماده ۶۹۸ قانون مجازات اسلامی است و به دو دلیل عمده با برخی تغییرات دیگر در فضای مجازی رایانه و اینترنت آورده شده است؛ اولا" وسیله ارتکاب جرم در ماده ۶۹۸ حصری است و شامل سیستم رایانه‌ای و مخابراتی نمی‌شود و حتی حقوقدانان با اختلاف آراء به سختی تلویزیون و رادیو را با توجه به تفسیر منطقی، داخل در این ماده می‌دانند و لازم بود تا تکلیف نشر اکاذیب در محیط سایبر نیز مشخص گردد. ثانیاً نشر اکاذیب جرمی است که در محیط سایبر بسیار شایع است. در این جا وسیله ارتکاب جرم بسیار مناسبتر و راحتتر در خدمت تحقق فعل فیزیکی جرم است. جرم موضوع ماده بر خلاف ماده ۶۹۸ دارای سوء نیت خاص نیست و در عوض مقید به حصول نتیجه است و نشر اکاذیب باید موجب تشویش اذهان عمومی یا مقامات رسمی یا غیر شود.

به لحاظ اینکه محیط سایبر ذاتاً برای نشر اکاذیب مناسب است و در واقع محیط تبادل اطلاعات است و برای تحقق رکن مادی نشر اکاذیب تشریفات مربوط به محیط واقعی لازم نخواهد بود، مجازات خفیف حبس از ۹۱ روز تا ۶ ماه در نظر گرفته شده است تا مشمول مجازات‌های اجتماعی شود و به مجازات متناسب دیگری تبدیل گردد و یا جزای نقدی دو میلیون و پانصد هزار تا ده میلیون ریال به این دلیل که مرتکب جرم رایانه‌ای معمولاً توان پرداخت جزای نقدی را دارد. در هر حال تعیین یکی از مجازات‌های حبس یا جزای نقدی اختیاری است. جرم موضوع این ماده به استثنای نشر یا در دسترس قرار دادن اکاذیب یا نسبت دادن اعمال خلاف حقیقت که موجب تشویش اذهان عمومی یا مقامات رسمی گردد به لحاظ اینکه در اینجا، جنبه عمومی جرم غلبه دارد، قابل گذشت است.

نشر اکاذیب رایانه ای برخلاف نشر اکاذیب سنتی، جرم مقید به حصول نتیجه محرمانه است .انتشار یا در دسترس قراردادن اکاذیب یا نقل قول برخلاف حقیقت باید منجر به یکی از دو نتیجه زیر شود: تشویش اذهان عمومی یا مقامات رسمی و ایراد ضرر به غیر. مقید و قبیح بودن جرم شرایط تحقق و اثبات آن را مشکل می‌سازد و این به دلیل شرایط و مقتضیاتی است که فضای سایبر فراهم ساخته است .

۶ـ مسئولیت کیفری ارایه دهندگان خدمات اینترنتی

ارایه دهندگان خدمات اینترنتی [۹] در مفهوم عام، عواملی هستند که به هرشکل اطلاعات و خدمات اینترنتی را در اختیار کاربران یا مشترکین قرار می‌دهند و شامل ایجاد کنندگان نقطه تماس بین‌المللی،[۱۰] ارایه دهندگان خدمات دسترسی[۱۱] ارایه دهندگان خدمات میزبانی[۱۲] و واسطین و عوامل مرتبط با آنها می‌شود.

پیش از این گفتیم که تولید یا ارایه یا انتشار محتویات غیر قانونی در فضای مجازی رایانه و اینترنت جرم و قابل کیفر است و قاعدتاً مسؤولیت کیفری بر کسی بار می‌شود که عناوین مجرمانه مربوط به محتویات رایانه‌ای را انجام دهد، اما چون دسترسی به اینترنت و خدمات آن از طریق ارایه دهندگان خدمات اینترنتی میسر می‌شود، این عوامل باید در برخی مواقع مسؤولیت کیفری ناشی از ارایه محتویات غیر قانونی را متحمل شوند. غیرقانونی بودن محتویات گاه به این دلیل است که قانون از آنها حمایت کرده و شخصی این حمایت قانونی را نقض نموده است؛ مثل محتویات متضمن نقض کپی رایت یا نقض حریم خصوصی و گاه غیرقانونی بودن محتویات، این دلیل است که قانون از آنها حمایت می‌کند، چون این محتویات ذاتاً غیر اخلاقی و نامشروع هستند، مثل محتویات هرزه یا محتویات، مسؤولیت دارند امّا در این جا منظور از مسؤولیت رساها، مسؤولیت در قبال محتویات ذاتاً غیراخلاقی و نامشروع است. ارایه دهندگان خدمات اینترنتی بر اساس مقررات و در حد متعارف مکلّف هستند از طریق تدابیری همچون پالایش، نصب باروری آتشین و .... از ارایه محتویات غیر قانونی تعریف شده در قانون، ممانعت به عمل آورند.[۱۳] مسؤولیت پالایش و ممانعت از ارایه محتویات غیر قانونی را می‌توان مسؤولیت پیشگیرانه یا مسؤولیت پیش از ارتکاب جرم نامید. این مسؤولیت در لایحه مجازات جرایم رایانه‌ای نیز پیش بینی شده است. به موجب ماده ۲۰ این لایحه، ایجاد کنندگان نقطه تماس بین‌المللی موظفند امکان دستیابی به محتویات موضوع ماده ۱۵ و بند الف ماده ۱۶ را متوقف سازند، در غیر این صورت به مجازات مقرر در ماده ۲۵ محکوم خواهند شد. سایر ارایه کنندگان خدمات اینترنتی نیز که با علم به تخلف اشخاص فوق خدماتی را دریافت و امکان دستیابی به این محتویات را فراهم ننمایند به مجازات فوق محکوم خواهند شد. مجازات مقرر در ماده ۲۵ لایحه، سه ماه و یک روز حبس یا جزای نقدی از دو میلیون و پانصد هزار تاده میلیون ریال است. بر اساس ماده۲۰ لایحه، ایجاد کنندگان نقطه تماس بین‌المللی موظّف به پالایش و توقف محتویات هرزه هستند و به لحاظ هزینه‌های گزاف نرم افزارهای پالایشگر و عدم امکان کامل پالایش محتویات غیر قانونی اولاً تکلیف پالایش فقط در مورد

9-Internt Service Provider (ISP
10-International Contact Point Or Internet Connection Provider(Icp)
11-Access Service Provider(Asp)
12- Hosting Service Provider(Hsp)

۱۳–پالایش یا فیلتر گذاری (Filtering) مهمترین اقدام درجهت قطع ارتباط بین کاربران و مشترکین با محتویات هرزه و غیرقانونی است که عمدتاً تضمن اقدام در ارتباط با محتویات، رایانه‌ای است :طبقه‌بندی محتویات ٌارزیابی محتویات و حذف آنها نصب نرم افزارهای مربوط به پالایش بر حسب کیفیت و کمیت عملکرد آنها، غالبا" متضمن هزینه‌های گزافی است.

محتویات مستهجن است و شامل محتویات غیرقانونی متضمن توهین، افترا، نشر اکاذیب که عمدتاً نوشتاری هستند، نمی‌شود و ثانیاً مسؤولیت فیلترگذاری فقط بر عهده ایجاد کنندگان نقطه تماس بین‌المللی است، نه سایر ارایه دهندگان خدمات اینترنتی و علت این امر این است که ایجاد کنندگان نقطه تماس بین المللی به لحاظ دولتی بودن یا به جهت دارا بودن امکانات کافی، موظَف به پیشگیری از ارایه و انتشار محتـــویات مستهجـــن شـــده‌اند و ایـــن شرایط در مورد سایر ارایه کنندگان خدمات اینترنتی به مراتب کم رنگ تر است.

در مورد مسئولیت پسینی یا مسئولیت پس از ارتکاب جرم، برای ارایه دهندگان خدمات اینترنتی بر فرض آگاهی و اطلاع از محتویات مستهجن یا غیر قانونی، سه نوع مسؤولیت کیفری مطرح می‌گردد:

الف) مسؤولیت کیفری مستقیم: چنانچه عملکرد ارایه دهنده خدمات اینترنتی، متضمن ارتکاب یکی از جرایم مرتبط با محتوا باشد، اعم از اینکه محتویات مستهجن باشند یا توهین آمیز، مستقلاً و مستقیماً مرتکب جرم تلقی می‌شود و مستوجب کیفری مندرج در مقرره مربوطه خواهد بود؛ به عنوان مثال اگر ارایه دهنده خدمات اینترنتی با علم و آگاهی، محتویات مستهجن موضوع ماده ۱۵ یا ۱۶ را انتشار دهد، به مجازات مقرر در این دو ماده حسب مورد محکوم خواهد شد.

ب) مسؤولیت کیفری ناشی از فعل غیر: در این قسم از مسؤولیت، ارایه دهنده خدمات اینترنتی به لحاظ عدم نظارت بر نحوه ارایه خدمات یا با توجه به منافعی که از ارتکاب جرم عاید آن می‌شود، در قبال ارتکاب جرم توسط دیگری مسؤولیت کیفری خواهد داشت، اعم از اینکه مرتکب جرم خود مسؤولیت کیفری داشته باشد یا نداشته باشد. در ارتباط با انتقال محتویات مبادله اطلاعات، ارایه دهندگان خدمات اینترنتی مخصوصاً ایجادکنندگان نقطه تماس بین‌المللی و ارایه‌دهندگان خدمات میزبانی موظف به نظارت بر آنها هستند و چنانچه در امر نظارت سهل انگاری یا بی مبالاتی نمایند ودیگری مرتکب انتشار محتویات غیر قانونی گردد، ارائه دهنده خدمات نیز دارای مسؤولیت کیفری خواهد بود .

ج) مسؤولیت مشترک: مسؤولیت مشترک ارایه دهنده خدمات اینترنتی با مرتکب جرم رایانه ای ممکن است از سه جهت مطرح گردد: معاونت در جرم، تسبیب در جرم در جائیکه مباشر نیز مسؤولیت دارد و دستور ارتکاب جرم رایانه ای . در این قسم از مسؤولیت بر خلاف مسؤولیت نیابتی یا مسؤولیت ناشی از فعل غیر، سوء نیت در ارتکاب جرم وجود دارد و بر خلاف مسؤولیت کیفری مستقیم، ارایه دهنده خدمات اینترنتی، فعل فیزیکی جرم را خود انجام نمی‌دهد.

قابل ذکر است که چون ارایه دهندگان خدمات اینترنتی عموماً شخص حقوقی محسوب می‌شوند و در فضای سایبر اشخاص حقوقی امکانات و موقعیتهای بیشتری برای ارتکاب جرائم رایانه‌ای یافته‌اند. مسؤولیت کیفری اشخاص حقوقی، در لایحه مجازات جرایم رایانه‌ای پیش بینی شد. ماده ۲۳ این لایحه مقرر می‌دارد: در موارد زیر چنانچه جرایم رایانه ای مندرج در این قانون تحت نام شخص حقوقی و در راستای منافع آن ارتکاب یابد، شخص حقوقی دارای مسؤولیت کیفری خواهد بود:

الف ـ هرگاه مدیر شخص حقوقی مرتکب یکی از جرایم مندرج در این قانون شود.

ب ـ هرگاه مدیر شخص حقوقی دستور ارتکاب یکی از جرایم مندرج در این قانون را صادر نماید و جرم به وقوع بپیوندد.

ج ـ هرگاه یکی از کارمندان شخص حقوقی با اطلاع مدیر یا در اثر عدم نظارت وی مرتکب یکی از جرایم مندرج در این قانون شود۰

دـ هرگاه مدیر در ارتکاب یکی از جرایم مندرج دراین قانون معاونت نماید.

هـ ـ هرگاه تمام یا قسمتی از موضوع فعالیت عملی شخص حقوقی به ارتکاب یکی ازجرایم موضوع این قانون اختصاص یافته باشد.

تبصره ۱: منظور از مدیر در این ماده هر شخصی است که اختیار نمایندگی یا تصمیم گیری یا نظارت بر شخص حقوقی را دارا می‌باشد.

تبصره ۲: مسؤولیت کیفری شخص حقوقی مانع مجازات مرتکب نخواهد بود .

تبصره ۳: کلیه فعالیتهای نهادهای دولتی که در راستای اعمال حاکمیت می باشد از شمول این ماده مستثنی خواهد بود. "

ماده ۲۴ لایحه نیز به ضمانت اجراهای کیفری اشخاص حقوقی مسؤول اشاره دارد. به موجب این ماده، اشخاص حقوقی موضوع ماده۲۳، باتوجه به شرایط و اوضاع واحوال جرم ارتکابی، میزان درآمد و نتایج حاصله از ارتکاب جرم به ترتیب ذیل محکوم خواهند شد:

الف ـ سه تا شش برابر حداکثر جزای نقدی جرم ارتکابی .

ب ـ چنانچه حداکثر مجازات حبس آن جرم تا پنج‌سال باشد: تعطیلی موقت شخص حقوقی از یک تا۹ ماه.

ج ـ چنانچه حداکثر مجازات حبس آن جرم بیش از پنج سال باشد تعطیلی موقت شخص حقوقی از یک تا سه سال و در صورت تکرار جرم منحل خواهد شد.

تبصره ۱ـ مدیر شخص حقوقی که مطابق بند۳ این ماده منحل می‌شود تاپنج‌سال حق تأسیس یا نمایندگی یا تصمیم گیری یانظارت بر شخص حقوقی دیگر را نخواهد داشت.

تبصره ۲ـ خسارات شاکی خصوصی از اموال شخص حقوقی جبران خواهد شد. در صورتی که اموال شخص حقوقی به تنهایی تکافو نکند، ما به التفاوت از اموال مرتکب جبران خواهد شد.

نتیجه گیری

جرایم مرتبط با محتوا یاجرایم محتوایی، قسمت سیاه فناوری اطلاعات است که معایب و نارسایی‌های آن را به تصویر می‌کشد. تبادل اطلاعات در فضای مجازی اینترنت و رایانه، بدون تبادل محتویات هرزه و غیر قانونی امکانپذیر نیست و گویی این محتویات هرزه و غیر قانونی است که در تمام زوایای فناوری اطلاعات رخنه پیدا کرده است. زدودن این زنگار سیاه که از تبادل محتویات غیر قانونی بر چهره صنعت فناوری اطلاعات نشسته است به دو طریق میسر است: نخست شناسایی ماهیت فضای سایبر و صنعت فناوری اطلاعات و اشراف بر بستری که محتویات غیرقانونی در آن جریان دارند و دوم اتخاذ تدابیر پیشگیرانه وسرکوبگر متناسب با فضای مجازی اینترنت و رایانه که به موجب آن اولاً با لحاظ قانونگذاریهای سابق و با التفات به خلوت افراد در محیط سایبر و تأمین محیط آزادیها حتی الامکان از جرم انگاری زاید اجتناب شود. ثانیاً با توجه به اینکه محیط مجازی رایانه و اینترنت دنیای جدیدی را پیش رو می‌نهد که ارتکاب جرایم در آن هم سریع صورت می‌گیرد و هم دارای جذبه است، حمایتهای بیشتری از افراد خاص و به ویژه اطفال و نوجوانان صورت بگیرد. ثالثاً علاوه بر مسؤولیت کیفری مرتکب جرم مرتبط با محتوا، مسؤولیت کیفری ارایه دهندگان خدمات اینترنتی و همچنین سایر اشخاص حقوقی پیش بینی گردد تا همگان برای سلامت و امنیت دنیای جدید سرباز شوند و در صورت تخلف بازخواست گردند.

☑ عنوان: تخریب و اختلال در داده‌ها و سیستمهای رایانه‌ای

☑ نویسنده: مهدی فضلی

(دانشجوی کارشناسی ارشد رشته حقوق جزا و جرم شناسی دانشگاه تهران – مجتمع آموزش عالی قم

به گفته زیگموند فروید روانشناس معروف، عالم رؤیا، دنیای تحقق یافتن امیال برآورده نشده انسانی است. اکنون باید بر این باور بود که چنین دنیایی، نه در رؤیا، که به واقع نیز ظهور یافته است. امروزه این دنیای سایبر است که به مراتب بهتر و خطرناکتر از عالم رؤیا، امروزه می‌تواند تحقق بخش امیال برآورده نشده افراد باشد."

چکیده

رایانه شگفت‌انگیزترین اختراع بشری طی سالیان اخیر است که هر روزه بر پیشرفت آن افزون می‌گردد. این محصول اعجاب انگیز تفکر بشری، افراد، موسسات و دولتها را شدیداً وابسته خود ساخته، در عین حال جوامع و به تبع آن دانش حقوق را نیز که محصول فرایندهای اجتماعی است، تحت تأثیر قرار داده است. از جمله معضلاتی که جوامع امروز با پیدایش رایانه با آن مواجه شده‌اند، جرایمی است که در این حیطه امن، مخفی، آزاد و بدون محدودیت تحقق می‌یابد. از بین بردن، اختلال و غیرقابل استفاده کردن داده‌ها، اختلال در کارکرد سیستم‌های رایانه‌ای و جرایمی که مقدمه آنها محسوب می‌شوند، همچون تولید، توزیع، انتشار و معامله برنامه‌های مخرب، از جمله جرایمی هستند که در محیط رایانه و خصوصاً شبکه‌های رایانه‌ای روبه گسترش چشم‌انگیز و شتاب آلودی دارد. غالب کشورها در راستای مبارزه با این جرایم، اقدام به وضع یا اصلاح قوانین کیفری نموده‌اند تا بتوانند در برابر این پدیده شوم که امنیتو قابلیت دسترسی داده‌ها و سیستم‌های رایانه‌ای را به مخاطره می‌افکند، به مبارزه برخیزند. در مقاله حاضر، سعی بر آن بوده که وضعیت حقوقی مباحث مربوطه به تخریب و ایجاد اختلال در داده‌ها و سیستم رایانه‌ای و نیز وضعیت قوانین کیفری جمهوری اسلامی ایران در این خصوص مورد بررسی قرار گیرد.

مقدمه

رایانه محصول حیرت‌انگیز تفکر بشری طی سالیان اخیر است که امروزه به نحوی شگفت‌انگیز وارد ساختار زندگی انسانها شده است. ورود این ماشین متفکر به عرصه حیات آدمی، اساس زندگی وی را دگرگون ساخته و معضلات ناشی از زندگی در جوامع انسانی را که نیازمند حفظ و دسترسی به اطلاعات گسترده و نیز تسریع در تبادل این اطلاعات است، با سرعت و دقتی بسیار بالا، مرتفع کرده است.

از سوی دیگر پیوند رایانه‌ها به هم در قالب شبکه‌های اطلاع‌رسانی، برشتاب گردش اطلاعات در جهان افـزوده و قابلیـت تحصیل اطلاعات را بسیار افزایش داده است. بدین ترتیب باید بر آن بود که چون دنیـای داده و رایانـه در عصـر اطلاعـات بـه نیازهای اطلاعاتی مردم، گروه‌ها و سازمان‌ها به سرعت پاسخ می‌دهد، این امر به نوعی موجب "وابستگی" جوامع انسانی به این دنیای نوین شده است که هر لحظه نیز بر این وابستگی افزوده می‌شود.

اکنون داده به عنوان جایگزینی مطمئن برای بسیاری از اطلاعات مورد نیاز عمل می‌کند کـه دقـت و تسـهیل در امـور را بسیار بالابرده است: بانکداری الکترونیکی سبب شده که افراد با استفاده از "داده‌های اعتباری" به جای هرگونه وسیله دریافت و پرداخت دیگر، به راحتی عملیات بانکی خود را انجام داده و به جای "پرداخت‌ها و دریافت‌هـای نقـدی"، از پرداخـت و دریافـت داده‌ای بهره ببرند؛ تجارت الکترونیک از طریق شبکه جهانی، امکان دریافت هر نوع کالا و خدماتی را که افراد به آن نیازمندند، در اندک زمان ممکن فراهم ساخته است؛ سازمانهای دولتی و خصوصی، از اسـناد الکترونیکـی بجـای اسـناد کاغـذی اسـتفاده می‌کنند، که علاوه بر اینکه فضای بسیار کمی اشغال می‌کند، هر لحظه نیز براحتی قابل دستیابی بوده و بدین ترتیب کارمنـدان سازمان و مراجعین را از سردرگمی و کارهای دست و پاگیر اداری رهانیده است.

از این رو پیشبرد تعاملات جهانی امروز که مبتنی بر فضای رایانه‌ای (Cyber Space) است، بدون استفاده از این ابزار کارآمد، تقریباً ناممکن به نظر می‌رسد. در واقع فناوری اطلاعات (IT)[1]، چنان با تار و پود زندگی اشخاص در هم آمیخته که نه تنها جدایی این محیط از زندگی آنها امری غیرقابل تصور می‌نماید، بلکه با پیشرفت ایـن فنـاوری، ایـن آمیختگـی و وابسـتگی لحظه به لحظه شدت یافته و ابعاد تازه و پیچیده‌تری نیز به خود می‌گیرد.

اجتماع نیز در مواجهه با این تحول فناوری، همچنانکه خود موجبات آن را فراهم ساخته، از سویی دیگر تأثیر نیز می‌گیرد. در واقع، استفاده از این دنیای جدید، تأثیری جدی و عمیق نیز بر تعاملات اجتماعی داشته است: کیفیت روابط اجتمـاعی افـراد، هرچند با بهره‌گیری از محیط‌های دیجیتالی بهتر و راحت‌تر شده، از سویی دیگر آنها را از دنیای فیزیکی خـود و از پهنـه روابـط اجتماعی سابق دور ساخته و بر کمیت روابط دیجیتالی افزوده است. بدین ترتیب دنیای سایبر، رفته رفته افراد را از محـیط‌هـای اجتماعی خود خارج ساخته و خصوصاً نسل جدید را به دنیای خود فرا می‌خواند. برای مثال، با ورود رایانه‌های شخصـی (PC)[2] به منزل افراد، آمار ساعاتی که مردم صرف دیدن سایت‌های مختلف، ارسال و دریافت نامه‌های الکترونیکی یا گپ‌های دوسـتانه می‌کنند، بسیار بیشتر شده و هر روز نیز بر میزان آن می‌افزاید.

دانش حقوق نیز محصول اجتماع و فرایندهای اجتماعی است. و اینگونه آمیختگی فوق‌العاده دنیای سایبر با زندگی افـراد، این دانش را نیز که رابطه تنگاتنگی با تحولات اجتماعی دارد، سخت درگیر کرده است.

دانش حقوقی، بیش از هر چیز، علم ایجاد نظم از طریق قواعد حقوقی است که با پیشرفت‌های اجتماعی، بایـد راه‌حلهـای جدیدی برای استقرار نظم در محیط‌های نوین ارائه دهد. فضای سایبر نیز که محیطی "مخفی، آزاد و نامحدود" است احتیاج به نظم دارد و اگر خلاف این باشد، هر "صفحه" از این محیط می‌تواند "صحنه" جرم و آشفتگی‌های بسیار باشد.

محیط سایبر محیطی "مخفی" است: امروزه مجرمین حیطه سایبر، از رایانه به عنوان کانونی مخفـی، امـن و مطمـئن در راستای رسیدن به مقاصد شوم خود بهره می‌گیرند. در واقع، حس پوشیده ماندن اعمال ارتکابی و عدم کشف آنهـا کـه ناشـی از

۱- Information Technology
۲- Private Computer

عدم نظارت دقیق و مؤثر بر محیط سایبر است و نیز این موضوع که آثار جرایم ارتکابی در این محیط، معمولاً باقی نمی‌ماند و همچنین امکان بسیار کم تعقیب مجرمین این حیطه که ناشی از طبع جهانی بودن این جرایم، است به طوری که امکان ارتکاب جرم را در گوشه‌ای از دنیا فراهم می‌آورد که نتیجه آن در سوی دیگری از جهان بوقوع می‌پیوندد و نیز این کاستی که هنوز مرجع و سازمانی جهانی به طور خاص مسؤول نظارت بر این محیط و مبارزه با جرایم ارتکابی در این حیطه نبوده و کشورها نیز راهکاری قوی و هماهنگ برای حل این معضل در پیش رو نگرفته‌اند، به بزهکاران این دنیای خیالی فراغ بال می‌دهد که به دور از دیدگان شماتت بار پلیس و مردم، خواسته‌های شریرانه خود را به راحتی به معرض اجرا بگذارند. به واقع اکنون باید دنیای سایبر را عالم تحقق خواسته‌ها و امیال تحقق نیافته افراد دانست که علاوه بر اینکه محیطی مخفی برای پوشیده نگاه داشتن اعمالی ارتکابی آنهاست، "محیطی آزاد" نیز هست: برای مثال انتشار تصاویر مستهجن افراد و خصوصاً کودکان در این محیط، در عین حالی که وسیله سودآوری برای ارائه کنندگان این تصاویر گشته، برای خواستاران ارضای غرایز جنسی نیز دنیای آزاد فراهم آورده که هر لحظه که خواستند می‌توانند به راحتی وارد این دنیای خیالی خود که چندی پیش دور از ذهن و رؤیا گونه می‌رسید شوند و تمایلات غریزی خود را فرو بنشانند. محیط سایبر، همچنین دنیایی آزاد برای کسانی است که قصد ایذاء و اضرار افراد را دارند: کلاهبرداری رایانه‌ای، جعل، پونوگرافی هویت، مزاحمت‌های رایانه‌ای، جرایم علیه حساب پست الکترونیک افراد، شنود و دسترسی غیرمجاز به داده‌ها و سیستم‌های رایانه‌ای اشخاص، سرقت اطلاعات و ... همگی از مصادیق جرایمی هستند که رایانه امکان ارتکاب آنها را بسیار افزایش داده است. در واقع اکنون برای ارتکاب جرم، صرفاً به یک رایانه و فرصتی برای ارتکاب جرم نیاز است.

همچنین دنیای سایبر، دنیایی "بدون محدویت" است: ابعاد مادی ندارد که بتوان آن رادر مکان محدود کرد و همچون پهنه‌های ناپیدای عالم خیال وسعتی بدون مرز دارد. اکنون با استفاده از تکنولوژیهای نوین، سعی بر آن است که در کوچکترین محیط مادی، بزرگترین دنیایی دیجیتالی را ایجاد کرد که حجم وسیعی از اطلاعات را درخود داشته باشد. این دنیاهای کوچک و در عین حال بسیار بزرگ، وقتی که به صورت شبکه نیز در می‌آیند، آنچنان پهنه وسیع و دور از تصوری را فراهم می‌آورند که از آن می‌توان به عنوان "کهکشان بی‌انتهای سایبر" نام برد.

طبق آمار، هر روزه هفت میلیون صفحه به صفحات سایت‌های اینترنتی افزده می‌شود[۳] که چنانچه این مطلب صحیح باشد، تصور نظارت بر این محیط بی‌گستره که هر روز بر فضای آن می‌افزاید، امری بسیار مشکل و بعید می‌نماید و دانش حقوق باید در پی راهکارهای جدیدی جهت کنترل این "دنیای بدون محدودیت" باشد.

موضوعات حقوقی مرتبط با این دنیای جدید را می‌توان از ابعاد مختلف حقوقی و کیفری مورد بررسی قرار داد. برای مثال موضوعات مختلفی نظیر بانکداری الکترونیکی، تجارت الکترونیکی، امضاهای الکترونیکی و اسناد الکترونیکی در حوزه حقوق خصوصی و موضوعاتی چون تقسیم‌بندی و تشریح خصوصیات جرایم رایانه‌ای، جرم‌شناسی و پیشگیری از جرائم رایانه‌ای در حوزه حقوق کیفری قابل بررسی است.

در حقوق کیفری جرایم رایانه‌ای، توجه به این نکته لازم است که ارائه یک تقسیم‌بندی دقیق از این جرایم کاری مشکل است. این امر را می‌توان ناشی از ۳ عامل عمده دانست: یکی عدم اتفاق نظر حقوقدانان در تقسیم‌بندی این جرایم، به طوری که

۳- روزنامه همشهری، شماره ۳۱۹۸، شنبه، ۲۶ مهر ۱۳۸۲، ص۲.

عده‌ای قائل به جرم‌انگاری در مواردی هستند که دیگران آن را جرم نمی‌دانند.[۴] دیگر بدیع و نو بودن مباحث مرتبط با جرایم رایانه‌ای است، بطوریکه برخلاف حقوق کیفری سنتی که مبانی آن طی قرون و اعصار و در چالش مباحث حقوقی بسیار شکل گرفته و ابعاد آن روشن شده، جرایم رایانه‌ای چند دهه‌ای بیشتر نیست که مطرح شده و از این رو مسائل جدید و ناگفته در این زمینه بسیار بوده و همین امر سبب عدم اتفاق نظر حقوقدانان در این خصوص گشته است.[۵] نمود این عدم اتفاق نظر را می‌توان در قوانین کشورهای مختلف و دسته‌بندی این جرایم مشاهده کرد که بسیار بیشتر از سایر حوزه‌های حقوق کیفری اختصاصی، نشانگر دیدگاه‌های مختلف فکری حقوقدانان است.

عامل دیگری که سبب این اختلاف نظرها شده، میزان وابستگی جوامع مختلف به محیط سایبر است: در جوامع پیشرفته که این وابستگی بیشتر است، جرم‌انگاری آن کشورها در این حیطه نیز گسترده‌تر است. و بالعکس در جوامع توسعه نیافته و در حال توسعه، به لحاظ میزان وابستگی کمتر آنها به این محیط، هنوز در بسیاری موارد ضرورت جرم‌انگاری مواردی که در کشورهای توسعه یافته، جرم رایانه‌ای محسوب می‌شود، احساس نشده و از این رو در قوانین کیفری آنها نیز نمود چندانی نداشته است. به همین لحاظ، برخی کشورها در حوزهٔ جرم انگاری در خصوص جرام رایانه‌ای، برخلاف کشورهایی که اقدام به وضع قوانین کیفری خاص و مستقل در این زمینه کرده‌اند، قوانین سنتی خود را بسنده دیده و برای پیدایش مسائل مستحدثه و جدید در این زمینه به قوانین موجود خود عطف داده‌اند.

در سطح بین‌المللی نیز تلاشهایی چند برای یکسان‌سازی موضوعات مرتبط با جرایم رایانه‌ای انجام شده است. در واقع طبع جهانی و خصوصیات خاصی که این جرایم دارند، ضرورت یکسان‌سازی مقررات این حیطه را بیشتر از سایر جرایم جهانی نمودار می‌سازد. از جمله این تلاشها می‌توان به کنوانسیون بوداپست شورای اروپا و مجموعه مقررات OECD[۶] اشاره کرد.

***

در مقاله حاضر موضوعات ذیل مورد بررسی قرار گرفته است:

۱) از بین بردن، اختلال و غیرقابل استفاده کردن داده‌های رایانه‌ای؛

۲) اختلال در کارکرد سیستم و شبکه‌های رایانه‌ای؛

۳) انتشار برنامه‌های مخرب در محیط سایبر.

و علاوه بر تشریح ابعاد حقوقی موضوعات فوق، در کنار آن به لحاظ تطبیقی، به مقررات برخی از کشورها و کنوانسیون بوداپست شورای اروپا نیز اشاره‌ای رفته است.

۴- برای دیدن اختلاف نظرها در طبقه بندی جرایم رایانه‌ای برای مثال ر.ک: مقاله Cyber Crime and Punishment، ص۳. سایت: (www.witsa.org/papers/McConnel Cybercrime.pdf) و نیز ر.ک مقاله Cyber laws:A Global Perspective، نوشته Manish Lunder،ص۲ سایت:(http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN/005846.pdf) ، نیز ر.ک سایت www.CyberCrime.net

۵- در واقع جرایم رایانه‌ای از دهه ۱۹۶۰ میلادی و پس از قضیه کلاهبرداری الدن رویس در آمریکا مطرح و مباحث آن مورد توجه حقوقدانان قرار گرفته است.

۶- Organization of Economic Co-operatioin and Development

محیط سایبر

واژه سایبر[۷](Cyber) ، چند سالی بیشتر نیست که توسط متخصصین فناوری اطلاعات مورد استفاده قرار می‌گیرد و در همین چند سال، آنچنان مقبولیتی یافته که غالباً از محیطهای دیجیتالی که با داده کار می‌کنند، با عنوان سایبر یاد می‌شود. در واقع واژه سایبر به کلیه محیطهایی اشاره دارد که اساس فعالیت آنها بر مبنای پردازش داده بوده و طبق سیستم صفر و یک کار می‌کنند.

عبارت رایانه (Computer)، به نحو دقیق و جامع نمی‌توانند گستردگی این محیط را نشان دهد، چه بسیاری از ابزار و وسایل امروزی با داده‌هایی کار می‌کنند که اساساً به آنها رایانه اطلاق نمی‌شود. از این‌رو به کاربردن عباراتی نظیر جرایم رایانه‌ای یا جرایم اینترنتی[۸] نیز نمی‌تواند به نحوی دقیق جرایم ارتکابی مربوط به این حوزه را پوشش دهد. برای مثال، یک سیستم ضبط و پخش صوتی دیجیتالی، رایانه نیست، اما به طور کلی در زیر مجموعه دنیای سایبر قرار می‌گیرد.

در لغت فارسی، واژه سایبر را به "مجاز و مجازی" ترجمه کرده‌اند. این ترجمه گویای دقیق عبارت سایبر نیست: مجاز که در برابر حقیقت به کار می‌رود، در زبان انگلیسی معادل واژهٔ "Virtual " است. از سوی دیگر، محیط سایبر، محیطی است حقیقی و واقعی و نه دروغین و مجازی. در واقع دنیای سایبر، هر چند به صورت مادی و ملموس قابل احساس نیست، اما همانطور که به اطلاعات حاصل از امری نمی‌توان صفت مجازی داد، به دنیای سایبر نیز نمی‌توان مجاز و مجازی اطلاق کرد. معهذا چون در زبان فارسی، واژه‌ای که مترداف با این عبارت باشد یافت نشده، استفاده از عبارت فضای مجازی[۹] و جرایم دنیای مجازی[۱۰] روبه گسترش است که رفته رفته جایگزین عباراتی چون جرایم رایانه‌ای و جرایم اینترنتی می‌گردد.

از محیط سایبر، به محیط فناوری اطلاعات (IT)[۱۱] یا محیط اطلاعات و ارتباطات (ICT)[۱۲] نیز یاد شده و از این رو مشاهده می‌شود که برای مثال از جرایم محیط سایبر، به جرایم علیه فناوری اطلاعات نیز نام برده می‌شود. عبارات مزبور، نیز نمی‌توانند به نحو جامع متضمن جرایم محیط سایبر باشند. چه برای مثال بسیاری از جرایم در محیط سایبر و با استفاده از این محیط صورت می‌گیرد و نه لزوماً "علیه" محیط سایبر و لذا عبارت جرایم علیه فناوری اطلاعات نیز عبارت صحیحی نخواهد بود. همچنین باید توجه داشت که فناوری اطلاعات تأکید بر "ابزار" دارد، حال آنکه سایبر به "محیطی" اشاره دارد که جرم در آن محیط بوقوع می‌پیوندد.

۷- واژه سایبر از عبارت سایبرنتیک (Cybernetics) مشتق شده که به معنی علم مطالعه سیستمهای کنترل مانند سیستم عصبی در موجودات زنده و توسعه سیستم‌های معادل آنها در وسایل الکترونیکی و مکانیکی است. سایبرنتیک، تفاوتها و تشابهات بین سیستمهای زنده و غیرزنده را مقایسه کرده و متکی به تئوریهای ارتباطی و کنترلی است که در هر دو زمینه قابل اجرا باشند. (فرهنگ تشریحی کامپیوتر، مایکروسافت،2003، ویرایش پنجم، ترجمه دکتر رضا حسنوی و مهندس داریوش فرسایی، انتشارات دانشیار، صص ۱۵۰ و۱۵۱). نیز ر.ک واژه Bionic، (همان، ص۶۷).

۸- Internet Crime

۹- Cyber Space

۱۰- Cyber Crime

۱۱- Information Technology

۱۲- Information Communication Technology

از بین بردن، اختلال و غیرقابل استفاده کردن داده‌ها

با اهمیت یافتن محیط‌هایی که امروزه با داده کار می‌کنند، باید بر آن بود که کشورها هر چه سریعتر باید در خصوص حمایت از داده‌ها اقدام به جرم‌انگاری کنند. اکنون، داده‌های حاصل از تلاش فکری و عملی متخصصین امور رایانه و کاربران این محیط، با کوشش و صرف هزینه‌های مالی و زمانی بسیار تولید می‌شود. از سوی دیگر حیات امروز جوامع بشری به نحوی شگفت با وجود این داده‌ها پیوند خورده است؛ چه در واقع داده‌ها جان رایانه بوده و کارکرد رایانه بدون داده ممکن نیست. آماری که هرساله توسط کشورهای مختلف ارائه می‌گردد، نشانگر این واقعیت است که از بین بردن داده‌ها در محیط‌های رایانه‌ای و خصوصاً در شبکه جهانی اینترنت، رشد فزاینده ای دارد که مثال بارز آن طراحی برنامه‌های مخربی است که از آنها با عناوینی چون ویروس، تروا و کرم‌های رایانه‌ای یاد می‌شود و هر ساله با انتشار در شبکه جهانی اینترنت سبب از بین رفتن مقادیر بسیاری از اطلاعات ارزشمند کاربران رایانه می‌گردد.[۱۳]

همچنین یکی از اهداف نفوذگران غیرمجاز به محیط سایبر که از آنها به عنوان هکر[۱۴] یاد می‌شود، در بسیاری موارد از بین بردن داده‌های دیگری است. شبکه‌های تروریستی نیز که قبلاً فعالیت‌های خود را با اعمالی چون کشتار افراد و تخریب اموال و اشیاء به انجام می‌رساندند، اکنون از این راه نوین که البته تبعات کمتری نسبت به اعمال فوق ندارد، برای رسیدن به اهداف خود و ضربه رساندن به مجموعه‌های مخالف بهره می‌گیرند. به طوری که تروریسم رایانه‌ای اکنون در کنار سایر اعمال تروریستی رفته رفته جایگاهی حائز اهمیت می‌یابد.[۱۵]

همچنین از بین بردن داده‌ها، مقدمه بسیاری از جرایم رایانه‌ای دیگر است. برای مثال جعل، کلاهبرداری رایانه‌ای یا اختلال درکارکرد سیستم ممکن است با از بین بردن و اختلال در داده‌های موجود تحقق یابد و از این رو خود به عنوان عملی که مقدمه جرایم دیگر قرار می‌گیرد صورت پذیرد.

از بین بردن، اختلال و غیرقابل استفاده کردن داده‌ها اعمالی هستند که تمامیت (Integrity) و قابلیت دسترسی (Availability) به داده‌ها را به خطر می‌افکنند. این امر سبب گشته که قسمتی از تلاش متخصصان فناوری اطلاعات، معطوف یافتن راهکارهای فنی مبارزه با شیوه‌های ارتکاب این جرایم گردد. از سوی دیگر خطر از بین رفتن داده‌های موجود در رایانه اشخاص، همواره آنان را وامی‌دارد که در جهت ایمنی سیستم‌های رایانه‌ای خود و نیز جهت پیشگیری از تحقق نتایج زیانبار حمله‌های رایانه‌ای که داده‌های آنان را از بین برده، مختل یا غیرقابل استفاده می‌سازد، از ابزارهای فنی ارائه شده توسط متخصصین این حرفه بهره گیرند و هر از چندی با بروز خطرات جدید آنها را روزآمد سازند. بدین ترتیب هزینه‌هایی که از راه

۱۳- برای مثال ر.ک گزارش جرایم و سوء استفاده رایانه‌ای هند در سال ۲۰۰۲-۲۰۰۱ Computer Crime & Abuse ،India، 2001-2002 Report در سایت (www.asianlaws.org/report0102.pdf) و نیز ر.ک گزارش CRS به کنگره آمریکا در سال ۲۰۰۳ (CRS Report Congres)،2003،March در سایت (http://fpc.state.gov)

۱۴- Hacker/Cracker

۱۵- برای مثال در این زمینه ر.ک مقاله تروریسم رایانه‌ای در بافت جهانی سازی نوشته روهاس ناگپال (Cyber Terrorism in the Context of Globalization) در سایت (www.ieid.org/congreso/ponensias/Nagpal/%2Rohas.pdf) و نیز ر.ک گزارش CRS به کنگره آمریکا درباره تروریسم رایانه‌ای CRS،Report Congress، ۱۹ ژوئن ۲۰۰۱ در سایت: (http://fpc.state.gov)

ارتکاب این جرایم بر کاربران و سازمان‌ها تحمیل می‌شود در مجموع مبالغ گزافی را در برمی‌گیرد[۱۶]. لذا وضع قاعده‌ای کیفری در سطحی جهانی توسط کشورها، برای مبارزه با این پدیده ضروری است.

از بین بردن، اختلال و غیرقابل استفاده کردن داده‌ها در قوانین ایران

در قوانین کیفری جمهوری اسلامی ایران، از بین بردن، اختلال و غیرقابل استفاده کردن داده‌ها فاقد وصف مجرمانه است.[۱۷] ماده ۶۷۷ قانون مجازات اسلامی نیز که اختصاص به تخریب، تلف و از کار انداختن، اشیاء منقول یا غیر منقول متعلق به دیگری دارد، نمی‌تواند موارد مزبور را تحت پوشش قرار دهد، چه چنانچه خواهد آمد، در بسیاری موارد (خصوصاً در مورد داده‌های دیجیتالی) نمی‌توان داده‌ها را شیء دانست.[۱۸] از سوی دیگر برای اختلال در داده‌ها یا غیرقابل استفاده کردن آنها نیز نمی‌توان عبارت تخریب یا از کار انداختن را به کار برد، چه در موارد مزبور داده‌ها از بین نرفته یا از کار نمی‌افتد و از این رو نمی‌توان آنها را تخریب یا از کارانداختن تلقی نمود. بدین ترتیب لزوم وضع قاعده کیفری مستقلی در ایران جهت حمایت از قابلیت دسترسی و تمامیت داده‌ها احساس می‌شود.

رفتار مجرمانه

از بین بردن، اختلال و غیرقابل استفاده کردن داده‌ها از سه طریق کلی قابل ارتکاب است:

۱) از طریق اعمال فیزیکی: نظیر شکستن دیسک یا تخریب دیسک سخت رایانه که حاوی داده‌اند، که سبب می‌شود داده‌ها از بین رفته یا غیرقابل استفاده شوند.

۲) از طریق سیستم رایانه‌ای: مثل اینکه با دادن فرمان حذف داده به سیستم رایانه‌ای، سیستم رایانه‌ای داده‌های وارد شده را پردازش و بر اساس آن، داده‌های موجود را حذف نماید.

۳) از طریق امواج: که با ارسال امواج، داده‌ها حذف، مختل یا غیرقابل استفاده می‌گردند.

۱- از بین بردن داده‌ها: از بین بردن داده‌ها واژه‌ای است که می‌توان آن را معادل تخریب در حقوق جزای سنتی دانست و از همین روست که از بین بردن داده‌ها را جزو جرایم رایانه‌ای خاص یا محض ندانسته‌اند. چه، از بین بردن و تخریب به طور سنتی از قدیم وجود داشته و اکنون نسبت به داده‌ها نیز اعمال می‌شود و لذا نمی‌توان آن را از جمله جرایمی دانست که صرفاً با روی کار آمدن محیط سایبر خلق شده باشند. معهذا باید توجه داشت که عبارت "تخریب "را در مورد داده‌ها به لحاظ ویژگی‌های

۱۶- برای مشاهده طرق و هزینه‌های ایمن‌سازی سیستم‌های رایانه‌ای در برابر حملات محیط سایبر ر.ک مقاله چگونگی جلوگیری از سابوتاژ سایبری How to Prevent Cyber Sabotage در سایت: www.giac.org/practical/GSEC/James_harris_GSEC.pdf و نیز ر.ک مقاله حمایت از سیستم‌های IT از جرایم رایانه‌ای (Protecting IT systems from Cyber Crimes) در سایت: www.CS.ncl.ac.ud/Research/Pubs/articles/paper/311.pdf

۱۷- مگر در مورد داده‌هایی که حالت فیزیکی دارند، مثل داده‌هایی که به شکل بارکد بر روی برخی کارتها وجود دارد.

۱۸- به توضیح شماره ۱۷ مراجعه شود.

خاصی که خصوصاً داده‌های دیجیتالی دارند، باید با مسامحه به کار برد و از این رو عبارت "از بین بردن داده‌ها" به نظر مناسب‌تر از عبارت "تخریب" است.[۱۹] معادل این واژه عبارات دیگری همچون امحاء، حذف و پاک کردن داده‌ها نیز به کار می‌رود که بیشتر عباراتی فنی هستند.

۲- اختلال در داده‌ها: اختلال در داده‌ها، ناظر به حالتی است که داده‌ها از بین نمی‌روند، بلکه دچار اختلال می‌شوند. در واقع در این حالت، داده‌ها موجودند، اما ترتیب منطقی آنها به هم می‌ریزد. این امر خصوصاً در مورد داده‌های دیجیتال و آنالوگ اتفاق می‌افتد.[۲۰] بدین ترتیب اگر کسی با اجرای یک برنامه خرابکارانه نسبت به داده‌ها، سبب شود که نظم و ترتیب آنها به هم ریزد، داده‌ها را مختل کرده است.

۳- غیرقابل استفاده کردن داده‌ها: این امر نیز ناظر به حالتی است که داده‌ها از بین نمی‌روند و همچنان وجود دارند، اما عملاً غیرقابل استفاده گشته و مشابه اصطلاحی که در حقوق مدنی به کار می‌رود، در حکم تلف قرار می‌گیرند. برای مثال اقدام شخصی که بر روی یک دیسک فشره (CD) که حاوی اطلاعات و داده‌های ارزشمندی است، خراشی وارد می‌آورد، به نحوی که داده‌های موجود در آن از بین نمی‌روند، اما سیستم رایانه‌ای دیگر قادر به پردازش (و به اصطلاح خواندن) داده‌های موجود در آن دیسکت نمی‌گردد را باید غیرقابل استفاده کردن آن داده‌ها دانست. همچنین، آنجا که کسی دیسکت دیگری را می‌شکند، در قسمتی که دیسکت شکسته است، داده‌ها از بین رفته‌اند، اما در سایر قسمت‌های آن دیسک که داده‌ها موجودند، داده‌ها غیرقابل استفاده شده‌اند.

موضوع جرم

موضوع جرم در هر یک از موارد از بین بردن، اختلال و غیرقابل استفاده کردن داده‌ها، داده است. داده (data) جمع عبارت لاتین datum به معنای یک قلم از اطلاعات است[۲۱]. در واقع داده را باید هر گونه مفاهیم، علایم، سیگنالها و اطلاعاتی دانست که توسط سیستم رایانه‌ای قابل پردازش است، به طوری که سیستم رایانه‌ای با دریافت آن اطلاعات و تجزیه و تحلیل منطقی، آن اطلاعات را درک کرده و به اصطلاح پردازش می‌کند. داده می‌تواند به اشکال مختلفی وجود داشته باشد: داده‌های آنالوگ موجود در نوارهای صوتی و تصویری، داده‌های موجود در دیسکت‌های فشرده (CD) (که به صورت سوراخ‌هایی بسیار ریزی است که بر سطح دیسکت ایجاد شده)، بار کدهای موجود بر روی یک کارت یا داده‌های دیجیتالی که در یک تراشه ذخیره شده و برای سیستم رایانه‌ای دارای مفهوم خاصی است و سیستم می‌تواند آن داده‌ها را پردازش کند.

داده ممکن است در سیستم رایانه‌ای بوده یا در حاملهای داده ذخیره شده باشد. منظور از حاملهای داده، ابزارهایی است که می‌توان داده‌های قابل پردازش سیستم رایانه‌ای را در آنها ذخیره کرد. بدین ترتیب یک دیسکت یا یک کارت دربردارنده داده های دیجیتالی یا فیزیکی یا حتی نوارهای ضبط و پخش صوتی و تصویری حامل داده محسوب می‌شود. همچنین امواج می‌توانند حامل داده باشند به طوری که داده‌ها در قالب سیگنالهایی، سوار بر آنها از نقطه‌ای به نقطه دیگر منتقل شوند.

۱۹- در واقع داده، هر گونه اطلاعات قابل پردازش در سیستم‌های رایانه‌ای است. و لذا چون در مورد اطلاعات به کار بردن واژه تخریب چندان مأنوس نیست، عبارت از بین بردن مناسب‌تر به نظر می‌آید.

۲۰- چون که این داده‌ها دارای ساختار سینوسی هستند و از این رو در معرض اختلال نیز می‌توانند واقع شوند.

۲۱- فرهنگ تشریحی کامپیوتر، همان،ص ۱۵۴.

داده همچنین ممکن است به صورت "ذخیره شده" یا "در حال جریان" باشد. لذا برای مثال داده‌های موجود در یک حامل داده، داده‌های ذخیره شده و داده‌های در حال انتقال در یک کابل نوری، داده‌های در جریان محسوب می‌شوند.

نتیجه جرم

از بین بردن، اختلال و غیرقابل استفاده کردن داده‌ها، جرمی مقید است که با اعمالی نظیر حذف و دستکاری داده‌ها و ورود ضرر به صاحب آن داده‌ها محقق می‌شود. معهذا نکته مهم در تحقق این جرم، قید ورود ضرر است که در این خصوص چند نکته قابل ذکر است:

– از بین بردن، اختلال و غیرقابل استفاده کردن داده‌ها، باید نسبت به داده‌های "معتبر" صورت گیرد. منظور از داده‌های معتبر، داده‌هایی است که قانوناً دارای ارزش هستند. در یک تقسیم‌بندی کلی، داده‌ها را به داده‌های مالی و داده‌های غیرمالی تقسیم می‌کنند. در واقع همهٔ داده‌ها دارای ارزش مالی نیستند و مفهوم مال را در حقوق مدنی ندارند، بلکه داده‌هایی مالی محسوب می‌شوند که مورد خرید و فروش قرار گرفته و اصطلاحاً دارای ارزش مبادله اقتصادی هستند. البته مراد این نیست که سایر داده‌ها، دارای ارزش نیستند. چه، ممکن است مورد خرید و فروش واقع نشوند ولی دارای ارزش شخصی باشند، مثل داده‌های تشکیل دهنده یک فایل شخصی که حاوی اطلاعات ذیقیمتی برای شخص است.

معهذا بسیاری از داده‌ها نیز فاقد ارزشند. برای مثال داده‌های یک برنامه ویروسی که برای از بین بردن فایل‌ها و اطلاعات دیگران برنامه‌ریزی شده، داده‌هایی بی‌ارزش است که مورد حمایت قانونی نیست و لذا از بین بردن و مختل کردن آنها به لحاظ اینکه داده‌های معتبری نیستند جرم محسوب نمی‌شود. در هر صورت ارزش داده‌ها، همچون ارزش سایر اموال نسبی بوده و با توجه به زمان و مکان تعیین می‌شود.

– در صورتی که داده‌ها از بین رفته، مختل یا غیر قابل استفاده شوند، باید میزان قابلیت بازیابی آنها را مدنظر قرار داد. برای مثال، چنانچه داده‌ها دارای منبع اولیه باشند، می‌توان داده‌ها را به سرعت و با همان کیفیت از آن منبع مورد بازیابی قرارداد، و بدیهی است ضرر وارده به داده‌های آسیب‌دیده‌ای که قابلیت جبران دارند مساوی با ضرری نخواهد بود که نسبت به داده‌هایی که غیرقابل بازیابی و جبران ناپذیرند، وارد می‌آید.

– از بین بردن، مختل کردن و غیرقابل استفاده نمودن داده‌ها باید به حدی باشد که عرفاً ضرری "عمده" محسوب شود و به اصطلاح، غیرقابل اغماض باشد. بدین ترتیب تخریب داده‌ها در حدی جزئی که به کلیت داده‌ها لطمه‌ای نزند را به این لحاظ که ضرر وارده چندان محسوس و قابل توجه نیست و عرفاً قابل اغماض است، نباید جرم دانست. تشخیص این امر بسته به مورد است و نمی‌توان قاعده‌ای کلی در این باره ارائه داد.

– داده‌ها،کلاً ویژگی آسیب‌پذیری بالایی دارند و بسته به جایگاهی که در آن ذخیره می‌شوند، ضریب ایمنی آنها متفاوت است. برای مثال ضریب ایمنی داده‌ها در دیسکت‌های فشرده، به مراتب کمتر از ضریب ایمنی داده‌هایی است که درون سیستم و در محفظه‌ای مطمئن قرار دارند.

قصد مجرمانه

از بین بردن، مختل کردن و غیرقابل استفاده کردن داده‌ها، همچون تخریب اشیاء و اموال در ماده ۶۷۶ قانون مجازات اسلامی، جرمی است عمدی؛ بطوری که فاعل باید هم قصد فعل ارتکابی را داشته وهم اینکه نتیجه را خواستار باشد.

معهذا ممکن است این اعتقاد وجود داشته باشد که در خصوص از بین بردن و اختلال در داده‌های مهم، همچون داده‌های دولتی، یا آنجا که شخص وظیفه نگهداری از داده‌ها را بر عهده دارد و بر اثر بی‌احتیاطی و بی‌مبالاتی داده‌های مهم را از بین برده یا مختل می‌سازد، اقدام به جرم‌انگاری گردد.

پذیرفتن این نظر از این جهت دارای ایراد است که هنوز داده‌ها بر اساس اهمیتشان تفکیک نشده‌اند و مشخص نیست که داده‌های مهم چه داده‌هایی هستند. از سوی دیگر این اعتقاد که داده‌های دولتی همواره دارای اهمیتند، امری بی‌اساس است. در واقع، این صحیح است که از دولت که به نفع عموم جامعه فعالیت می‌کند، باید حمایت بیشتری به عمل آید، اما این هم درست نیست که تمامی داده‌های متعلق به دولت را مهم فرض کرده و برای از بین بردن آنها مجازات وضع کنیم. معهذا شاید این امر در مورد داده‌های متضمن اطلاعات سری و محرمانه که دارای ویژگی خاص و مهمی هستند، به شرطی که مقررات مربوط به طبقه‌بندی این داده‌ها و طرز نگهداری آنها همچون سایر اسناد و اطلاعات طبقه‌بندی شده تنظیم شود، مورد قبول باشد.

ایجاد اختلال در کارکرد سیستم رایانه‌ای

از جمله اصول مهمی که در استفاده از یک سیستم رایانه‌ای باید همواره مدنظر باشد، حق بهره‌برداری صحیح از آن است، به طوری که کاربران باید برای دستیابی به اطلاعات موجود در سیستم رایانه‌ای، از کارکرد صحیح سیستم بهره‌مند باشند. چه، سیستم رایانه‌ای به منزله مظروفی است که داده‌ها و اطلاعات رایانه‌ای کاربران درون آن مستقر است و بدون کارکرد صحیح آن، بهره‌برداری از اطلاعات میسر نخواهد بود.

ایجاد اختلال در کارکرد سیستم رایانه‌ای از شیوه‌هایی است که امروزه بزهکاران محیط سایبر از آن به مقاصد مختلف بهره می‌گیرند و در واقع قابلیت دسترسی[۲۲] افراد را به اطلاعات با اختلال مواجه می‌سازند. برای مثال شخصی که با وارد کردن یک ویروس یا تروای رایانه‌ای به سیستم رایانه‌ای دیگری سبب می‌شود که کامپیوتر وی به طور خودکار روشن و خاموش گردد، موجب اختلال در کارکرد سیستم رایانه‌ای وی گشته است.

با پیدایش شبکه‌های رایانه‌ای، ایجاد اختلال در کارکرد سیستم رایانه‌ای نیز با بهره‌گیری از شبکه روبه فزونی گذاشته که همچون تخریب و اختلال داده‌ها، هر ساله خسارات هنگفتی بر دولتها، سازمانها و افراد وارد می‌آورد. به طوری که برای مثال، قطع ارتباط اینترنتی افراد یا اختلال در سرورهای (Server) ارائه کنندگان خدمات اینترنتی، امروزه از جمله حملات شایع رایانه‌ای در سطح شبکه‌های اطلاع‌رسانی کامپیوتری محسوب می‌شود.[۲۳]

۲۲- Availibility

۲۳- برای مثال ارسال حجم بسیار بالای داده به سرورهای ارائه‌کنندگان خدمات اینترنتی به طوریکه سرورها ظرفیت لازم برای دریافت، ذخیره و انتقال آن حجم داده را نداشته و از کار بیفتند از مصادیق اختلال در کارکرد سیستم رایانه‌ای محسوب می‌گردد.

اختلال در کارکرد سیستم رایانه‌ای در قوانین ایران:

در قوانین کیفری ایران، صراحتاً جرمی با عنوان اختلال در کارکرد سیستم رایانه‌ای پیش‌بینی نشده است. معهذا در این مورد شاید بتوان به عبارت "از کارانداختن" در مواد ۶۷۷ و ۶۸۷ قانون مجازات اسلامی استناد کرد. چنانچه می‌دانیم، ماده ۶۷۷ قانون مزبور ناظر به تخریب، تلف و از کار انداختن اشیاء منقول متعلق به دیگری است. همچنین ماده ۶۸۷ این قانون نیز اختصاص به تخریب، ایجاد حریق، "از کارانداختن" و هر نوع خرابکاری دیگر دارد که نسبت به وسایل و تأسیسات مورد استفاده عمومی از قبیل شبکه‌های آب و برق و تلفن و گاز و ... صورت می‌گیرد.

در واقع اگر بر این باور باشیم که عبارت "از کار انداختن" در مواد مزبور، متضمن معنای ایجاد اختلال نیز هست، لذا باید بر آن بود که مواد مزبور می‌توانند اختلال در کارکرد سیستم رایانه‌ای افراد را نیز پوشش دهند، چرا که عبارت "از کار انداختن" در مواد مزبور به طور منطقی ناظر به وسایل، تأسیسات و اشیایی است که "کارکردی" دارند و در کارکرد آنها، اختلالی ایجاد می‌شود، که می‌تواند موقتی یا دائم باشد.

اینگونه تفسیر مواد مزبور ممکن است از دو جهت مورد ایراد واقع شود: اول اینکه مقنن در مواد ۶۷۷ و ۶۸۷ قانون مجازات اسلامی، با آوردن عبارات اشیاء و وسایل و تأسیسات، نظر به حالتی داشته که با تخریب و تلف مادی اشیاء و وسایل، آن وسایل و اشیاء از کار بیفتند. و ثانیاً اینکه عبارت از کارافتادن، ناظر به حالتی است که کارکرد وسایل و اشیاء مزبور به طور دائم متوقف می‌شود و لذا "اختلال" را که از کارافتادن موقت تلقی می‌شود نباید "از کارافتادن" دانست.

معهذا ایرادات مزبور چندان قوی نیست که بتوان ایجاد اختلال در کارکرد سیستم‌های رایانه‌ای را از شمول آنها خارج کرد و لذا باید بر آن بود که این مورد نیز تحت پوشش مواد مزبور قرار می‌گیرد.

رفتار مجرمانه

ایجاد اختلال در کارکرد سیستم‌های رایانه‌ای، به سه طریق ممکن است:

۱) فعل فیزیکی: به طوری که شخصی با تخریب قسمتی از سیستم رایانه‌ای سبب شود که کارکرد آن با اختلال مواجه شود. بدیهی است این مورد را به طور خاص نمی‌توان جرم سایبری نامید.

در این حالت، اختلال در کارکرد سیستم خود از ۳ طریق متصور است:

– وارد کردن و انتقال داده‌ها؛

– متوقف کردن داده‌های در حال جریان؛

– پاک کردن، از بین بردن، دستکاری، اختلال و غیرقابل استفاده کردن داده‌ها.

۳) از طریق امواج: به طوری که با ارسال امواج کارکرد سیستم رایانه‌ای افراد مختل شود.[۲۴]

سیستم رایانه‌ای:

۲۴– بدیهی است در این حالت چنانچه امواج، خود حامل داده باشند و به وسیله داده‌ها این کار صورت گیرد، مورد مشمول حالت دوم خواهد بود.

سیستم را مجموعه‌ای از عناصر که برای انجام کار خاصی با هم کار می‌کنند، تعریف کرده‌اند. سیستم رایانه‌ای، خود متشکل از دو سیستم سخت‌افزاری و نرم‌افزاری است که در تعامل با یکدیگر، موجب کارکرد و فعالیت سیستم رایانه‌ای می‌شوند. سیستم سخت‌افزاری رایانه، متشکل از قطعاتی چون ریزتراشه، مدار، دستگاه‌های ورودی و خروجی و دستگاه‌های جانبی است. سیستم نرم‌افزاری رایانه نیز از مجموع برنامه‌ها و فایل داده‌ها تشکیل شده و یا در یک سیستم مدیریت بانک اطلاعاتی، برای پردازش انواع خاصی از اطلاعات به کار می‌رود.[۲۵]

نکته‌ای که باید بدان توجه داشت این است که در واقع نتیجه ایراد صدمه و تخریب به سیستم سخت‌افزاری سیستم رایانه‌ای، اختلال در کارکرد سیستم نرم‌افزاری و به طور کلی کارکرد سیستم می‌شود. در عین حالی که این امر، تخریب فیزیکی اشیاء نیز محسوب می‌شود.

نتیجه جرم:

ایجاد اختلال در کارکرد سیستم رایانه‌ای جرمی است مقید که با ایجاد هر گونه اختلال در عملکرد سیستم رایانه‌ای محقق می‌شود و باید قید ورود ضرر را نیز مدنظر قرار داد.

در واقع نکته‌ای که باید به آن توجه داشت این است که ایجاد اختلال در کارکرد سیستم رایانه‌ای باید به حدی باشد که عرفاً اختلالی عمده محسوب شده و غیرقابل اغماض باشد. بدین ترتیب ایجاد اختلالات جزئی در کارکرد سیستم رایانه‌ای که به اساس کارکرد سیستم لطمه‌ای جدی وارد نیاورد و عرفاً امری جزئی تلقی شود، بطوری‌که نتوان فرض ورود ضرر قابل توجهی را متصور دانست، نباید جرم باشد. تشخیص این امر حسب مورد متفاوت است و نمی‌توان قاعده‌ای کلی برای آن ارائه داد.

قصد مجرمانه

ایجاد اختلال در کارکرد سیستم رایانه‌ای جرمی است عمدی و برخلاف آنچه که در بحث از بین بردن و اختلال داده‌ها عنوان شد، تصور جرم‌انگاری در مورد حالتهای غیرعمد، حتی در مورد سیستم‌های رایانه‌ای حساس نیز چندان قابل قبول به نظر نمی‌رسد.

تولید و انتشار برنامه‌های مخرب و موجد اختلال

ایجاد شبکه‌های اطلاع‌رسانی رایانه‌ای در سطح جهانی عملیات تخریب و اختلال را نسبت به داده‌ها و کارکرد سیستم رایانه‌ای افراد بسیار تسهیل کرده است. این امر از سویی سبب شده که تولید و انتشار برنامه‌های ویرانگر و مختل کننده داده و سیستم با سرعتی بسیار زیاد رو به فزونی گذارد، و از سوی دیگر موجب آن شده که عده‌ای اساساً فعالیت خود را در راه ایجاد، تولید و توزیع چنین برنامه‌های مخربی (چه در سطح شبکه و چه در خارج از آن)، معطوف کرده و چه بسا به عنوان یک حرفه از این راه به کسب درآمد بپردازند.

۲۵- فرهنگ تشریحی کامپیوتر، همان، صفحه ۵۶۰.

آماری که هر ساله کشورهای مختلف درباره میزان خسارات وارده به بخش‌های مختلف دولتی، خصوصی، اقتصادی و اجتماعی خود ارائه می‌دهند، مبین این امر است که روند بهره‌گیری از شبکه برای تخریب و اختلال داده‌ها و سیستم رو به فزونی شتاب آلودی دارد.[۲۶]

بدین ترتیب این امر سبب شده که بسیاری از کشورها، نه تنها در حوزه تخریب و اختلال در داده‌ها و کارکرد سیستم رایانه‌ای خود، اقدام به وضع قوانین کیفری نمایند، بلکه برای پیشگیری از تولید، توزیع، معامله و انتشار این گونه برنامه‌های ویرانگر نیز مستقلاً اقدام به جرم‌انگاری نمایند.

این امر خود دو حوزه را تحت پوشش قرار می‌دهد:

۱) واردکردن و انتشار برنامه‌های مخرب و موجد اختلال در سطح شبکه، اعم از اینکه این کار به نتیجه تخریب و اختلال منجر گردد یا خیر.

۲) تولید، توزیع و معامله برنامه‌های مزبور اعم از اینکه در خارج از محیط شبکه باشد یا در سطح شبکه.

بدین ترتیب جرم‌انگاری در این زمینه که بیشتر در راستای پیشگیری از نتایج مخرب این اقدامات صورت گرفته، هر دو محیط خارج از فضای سایبر و محیط داخل آن را شامل می‌گردد. بدین ترتیب برای مثال وارد کردن یک ویروس مخرب در سطح شبکه جرمی است که در فضای سایبر و شبکه‌های رایانه‌ای اتفاق می‌افتد. معهذا فروش همان برنامه مخرب در قالب یک دیسکت یا حتی فروش آن در شبکه به دیگران نیز جرم است، چراکه قابلیت ایجاد همان میزان خطر را برای داده‌ها و سیستم‌های رایانه‌ای دارد.

برخی از این برنامه‌ها و حملات ذیلاً مورد بررسی قرار می‌گیرد:

۱- ویروس‌های کامپیوتری:[۲۷]

ویروس کامپیوتری، برنامه‌ای رایانه‌ای است که می‌تواند سایر برنامه‌های رایانه‌ای را با ایجاد تغییر در آنها، به صورتی که سبب می‌شود برنامه‌های رایانه‌ای دیگر یک کپی از آن ویروس را داشته باشند، تحت تأثیر قرار می‌دهد.[۲۸] در واقع ویروس رایانه‌ای، برنامه‌ای است که فایلهای کامپیوتر را با اضافه کردن کپی‌هایی از خود در آنها آلوده می‌کند. این کپی‌ها وقتی که فایل در حافظه بارگذاری می‌شود اجرا می‌شوند و می‌توانند فایل‌های دیگر را آلوده کنند. ویروس‌ها غالبا اثرات جانبی مخربی دارند (اما گاهی نیز بی‌ضررند). برای مثال برخی از این ویروسها می‌توانند به داده‌های موجود در دیسک سخت کامپیوتر ضرر برسانند یا حافظه‌ای را اشغال کنند که برای منظورهای دیگر، مورد نیاز برنامه‌هاست.[۲۹]

ویروس‌ها از آن جهت خطرناکتر می‌شوند که پیش از آن که بتوان آنها را متوقف کرد با سرعت بسیار منتشر می‌شوند و از این رو چون نمی‌توان جلوی پیشروی آنها را گرفت، سبب خسارات هنگفتی به داده‌ها و سیستم رایانه‌ای کاربران می‌شوند.

۲۶- ر.ک گزارش: Computer Crime & abuse Report، Indidia، 2001-2002 ، همان و نیز گزارش: CRS Report Congres، همان.

۲۷- Computer Viruses

۲۸- Cyber Terrorism in the Context of Globalization، همان.

۲۹- فرهنگ تشریحی کامپیوتر، همان، صفحه ۶۱۴

در طول مدتی که شبکه‌های رایانه‌ای مورد استفاده واقع می‌شوند، هزاران ویروس رایانه‌ای اطلاعات افراد را از بین برده یا سبب اختلال در کارکرد سیستم رایانه‌ای آنها شده‌اند که از آن جمله می‌توان به ویروس ملیسا[۳۰]، اکسپلورزیپ[۳۱]، چرنوبیل[۳۲]، دوستت دارم[۳۳]، مغز پاکستانی[۳۴]، Stoned-Marjuana[35]، آبشار[۳۶] و میکل آنژ[۳۷] اشاره کرد.

تراواها[۳۸]:

در قرن دوازدهم قبل از میلاد، دولت یونان به این خاطر که شاهزاده شهر تراوا (Troy)، ملکه اسپارت را برای اینکه به همسری برگزیند، می‌رباید، اعلام جنگ می‌کند. نیروهای یونانی به مدت ۱۰ سال شهر تروا را محاصر می‌کنند، اما به این خاطر که شهر مزبور از برج و باروی مستحکمی برخوردار بوده به موفقیتی نائل نمی‌شوند. آخرالامر نیروهای یونان ظاهراً آماده عقب‌نشینی شده و بارها کردن یک اسب چوبی بزرگ آنجا را ترک می‌کنند. مردم شهر تراوا با دیدن اسب مزبور و با این تصور

۳۰- Melissa، این ویروس در ۲۶ مارس ۱۹۹۹ شناسایی شد که در آن زمان سریعترین ویروسی بود که در کل شبکه جهانی منتشر شد. این ویروس به خودی خود بی‌ضرر بود و صرفاً در مواقع خاصی از روز عباراتی چند را به اسناد الکترونیکی اضافه می‌کرد. آما آنچه موجب حداکثر ضرر وارده توسط این ویروس گردید این بود که این ویروس خود را به آدرس پست‌الکترونیکی موجود در دفترچه آدرس قربانیان خود می‌فرستاد و بدین ترتیب با افزودن متن جدیدی به متن نامه‌های الکترونیکی افراد در سطحی کلی، حجم وسیعی از داده را ایجاد می‌کرد که این امر سبب گردید در آنزمان بسیاری از سرورها (Server) در کل جهان از کار بیفتد (Cyber Terrorism in the Context of globalization، همان، صفحه ۶).

۳۱- ExploreZip، این ویروس که در ژوئن ۱۹۹۹ شناسایی شد، در عین حالی که Microsoft Outlook کامپیوتر افراد را از کار می‌انداخت، برخی از فایلها را نیز انتخاب کرده و اندازه آنها را به صفر می‌رساند و چنین نشان می‌داد که هیچ‌گونه داده‌ای در آن فایلها وجود ندارد. بدین ترتیب داده‌های موجود در آن فایلها بلااستفاده شده و قابل بازیابی نیز نبودند (منبع پیشین، همان صفحه).

۳۲- Chernobyl، ویروس چرنوبیل یا ویروس PE CIH هر سال در روز ۲۶ آوریل (سالگرد فاجعه هسته‌ای چرنوبیل اوکراین) فعال می‌شود. این ویروس اولین مگابایت داده را از دیسک سخت کامپیوترهای شخصی پاک کرده و باقیمانده فایلها را نیز غیرقابل استفاده می‌نماید. این ویروس همچنین داده‌های موجود در تراشه سیستم اصلی ورودی و خروجی (BIOS) را حذف کرده و تا زمانی که تراشه جدیدی نصب نشود یا داده‌های موجود در تراشه قبلی مورد بازیابی قرار نگیرد، کامپیوتر را از کار می‌اندازد. خوشبختانه تنها BIOSهایی که قابل جایگزینی‌اند با خطر این ویروس مواجه می‌شوند.

۳۳- I Love You، این ویروس خطرناک در می سال ۲۰۰۰ شناسایی گردید و در آن زمان از هر پنج کامپیوتر شخصی در سطح جهان، یکی را تحت تأثیر قرار داد که خسارات ناشی از انتشار این ویروس در ایالات متحده بالغ بر ۱۰ بیلیون دلار گردید. این ویروس از آدرس قربانیان در Microsoft Outlook استفاده کرده و خود را به آدرس پست الکترونیکی آنها می‌فرستاد. بدین ترتیب نامه‌هایی با عنوان دوستت دارم به اشخاصی ارسال می‌کرد که سبب می‌شد افراد با گشودن آن نامه الکترونیکی، سبب ورود خسارت عمده‌ای به کامپیوتر خود گردند. ویروس مزبور برخی فایلها را انتخاب کرده و کد خود را به جای داده اصلی موجود در فایل وارد می‌کرد و بدین نحو هر لحظه به تعداد کپی‌های خود می‌افزود. (منبع پیشین، همان صفحه).

۳۴- Pakistani Brai، ویروس مزبور، اولین ویروسی شناخته شده‌ای است که در سطح جهانی منتشر شده است. (منبع پیشین، همان صفحه).

۳۵- ویروس مزبور در نیوزیلندایجاد شده و به این ترتیب عمل می‌کند که با ارسال مرتب پیامی با این مضمون که "کامپیوتر شما قفل شده. ماری جوانا را قانونی کنید" سبب اختلال در کارکرد سیستم رایانه‌ای می‌گردد.

۳۶- Cascade، این ویروس که همچنین Falling Letters یا ویروس 1701 نیز نامیده می‌شود، برای خاموش کردن کلید Numlock بر روی صفحه کلید کاربران عمل کرده و در عین حال عبارات موجود بر روی صفحه نمایشگر افراد را به صورت یک توده درآورده و به پایین صفحه انتقال می‌دهد. (منبع پیشین، همان صفحه).

۳۷- Michelangelo، این ویروس به نام هنرمند معروف ایتالیایی دوره رنسانس، میکل آنژ بوناروتی نامگذاری شده و هر ساله در روز ششم مارس، روز تولد این هنرمند، فعال می‌شود. (منبع پیشین، همان صفحه).

۳۸- Trojans

که اسب مزبور هدیه‌ای از یونانیان است، آن را به داخل شهر می‌کشند، غافل از اینکه درون اسب چوبی مزبور توخالی بوده و پر از بهترین جنگاوران یونانی است. سربازان یونانی در پناه شب از اسب پیاده شده و با گشودن درب‌های شهر و با کمک باقی سربازانی که در خارج منتظر بودند، تمامی ارتش تروا را از پای در می‌آورند.

در علوم رایانه‌ای نیز، اسب تروا مشابه اسب معروف در افسانه مزبور، برنامه‌ای است که ظاهراً خوب و مفید به نظر می‌رسد، اما در باطن متضمن برنامه‌هایی مخرب و مختل کننده است.[۳۹] اسب‌های تراوای رایانه‌ای انواع و اقسام بسیاری دارند که از آن جمله می‌توان به اسب‌های تروای اداره از راه‌دور[۴۰]، تروا‌های گذر واژه[۴۱]، تراواهای Key Loggers[۴۲]، Priviliges-Elevating[۴۳] و تراواهای مخرب[۴۴]، اشاره کرد.

کرم‌های کامپیوتری:[۴۵]

این واژه در ارتباط با رایانه، اولین بار توسط جان برونر،[۴۶] نویسنده کتابهای علمی تخیلی و در کتاب Shock wave Reader، مورد استفاده قرار گرفته است[۴۷].

کرم کامپیوتری، برنامه‌ای است که خود را در سیستم پخش می‌کند و معمولاً این عمل را با ایجاد کپی‌هایی از خود در حافظه کامپیوتر انجام می‌دهد. این برنامه ممکن است خود را در یک برنامه کپی کند که اغلب موجب از کار افتادن کامپیوتر می‌شود. گاهی نیز این برنامه در قطعه برنامه‌های مستقلی نوشته می‌شود که به اطلاعات صدمه وارد کرده یا آنرا از بین می‌برد.[۴۸]

۳۹- منبع پیشین، ص۵.

۴۰- Remote Adimnistration Trojans، تراواهای مزبور، به هکرها (Hacker) یا نفوذگران غیرمجاز به سیستم رایانه‌ای افراد، اجازه می‌دهد که به دیسک سخت رایانه قربانیان خود دسترسی یابند و همچنین اعمال دیگری نظیر کپی فایلها، خاموش کردن کامپیوتر و باز کردن و بستن خودکار محل قرار گرفتن CD-ROM را سبب می‌شود. (منبع پیشین، ص۵)

۴۱- Pasword Trojans تراواهای مزبور، رایانه قربانیان را برای یافتن گذر واژه‌ها جستجو کرده و آنها را به نویسنده برنامه ارسال می‌دارند. برای هر نوع گذر واژه‌ای، تراوای مخصوصی وجود دارد. این قبیل تراواها معمولاً اطلاعات را از طریق پست الکترونیکی افراد به مهاجم ارسال می‌دارند. (منبع پیشین، ص۵)

۴۲- این تراواها اطلاعاتی را که افراد از طریق صفحه کلید خود وارد رایانه می‌سازند (همچون گذر واژه‌ها) را ثبت کرده و با ذخیره آنها در یک فایل یا در پست الکترونیکی، آنها را به شخص مهاجم ارسال می‌دارند. این تروا‌ها فضای زیادی از دیسک را اشغال نکرده و به عنوان فایلهایی مفید، ذخیره شده و از این نظر کشف آنها بسیار مشکل است. (منبع پیشین، ص۵).

۴۳- این تراواها معمولاً مدیر سیستم (System Administrator) را که شخصی است که بر شبکه نظارت و تسلط دارد به اشتباه می‌افکند، به طوری که این تراواها با بی‌خطر و حتی مفید جلوه دادن خود سبب می‌شوند، مدیر شبکه آنها را گشوده و همین امر سبب می‌شود که خود مهاجم همچون مدیر شبکه، بر شبکه تسلط یابد.

۴۴- Destructive Trojans، این تراواها می‌توانند کل اطلاعات موجود در دیسک سخت قربانیان را از بین برده یا فایلهای مهم را رمزگذاری کرده یا از بین برده و غیرقابل استفاده سازند. (منبع پیشین، ص۵).

۴۵- Computer Worms

۴۶- John Bruner

۴۷- منبع پیشین، ص۷.

۴۸- فرهنگ تشریحی کامپیوتر، همان، صفحه ۶۳۷.

کرمهای رایانه‌ای معمولاً در شبکه مورد استفاده قرار می‌گیرند و بر خلاف ویروس‌های رایانه‌ای نیازی به اینکه خود را بـه یـک رایانه میزبان وصل کنند ندارند. کرمهای رایانه‌ای به دو دسته کلی تقسـیم بنـدی مـی‌شـوند: کـرم‌هـای کـامپیوتر میزبـان [۴۹] وکرمهای شبکه[۵۰]. کرمهای نوع اول در حافظه کامپیوتری که روشن است قرار گرفته و از شبکه برای ایجاد کپی هایی از خـود در کامپیوترهای دیگر استفاده می‌کنند و منبع اصلی پس از استقرار یک کپی برروی کامپیوتر میزبان، خود از بین می‌رود. لـذا در این حالت، صرفاً یک کپی از برنامه در لحظه خاصی از زمان در شبکه اجرا می‌شود.[۵۱]

اما کرمهای نوع دوم از قطعات (Segment) متعددی تشکیل شده‌اند که هریک از این قطعات در سیستم‌های مختلفی اجرا می‌شوند (و ممکن است هریک عملکردخاصی داشته باشند)، و از شـبکه بـرای اهـداف ارتبـاطی متعـددی بهـره می‌گیرند.[۵۲]

امروز در جهان، کرم‌های رایانه‌ای بسیاری در سطح شبکه وجود دارد که از مهمترین آنها می‌توان به کرم اینترنت[۵۳]، کـرم اسپان[۵۴] و کرم درخت کریسمس [۵۵] اشاره کرد.

حملات DoS[۵۶] و DDoS[57]

حملات DoS اساساً به منظور محروم کردن افراد از دسترسی صحیح و مستمر به سیستم‌هـای رایانـه‌ای خـود صـورت می‌گیرند و در صورتیکه این حملات به صورت گسـترده و در سـطح شـبکه اتفـاق بیفتـد از آن بـه حمـلات DDoS تعبیـر

۴۹- Host Computer Worms

۵۰- Network Computer Worms

۵۱- به این کرمهای شبکه همچنین Rabbits نیز اطلاق می شود. منبع پیشین، ص۷.

۵۲- به کرمهای شبکه‌ای که حاوی یک قطعه عمده بوده و کار دیگر قطعات را هماهنگ می‌سازند، اختاپوس(Octopuses) نیز نامیده می‌شـوند. منبـع پیشین، ص۷.

۵۳- Internet Worm ، در ۲۲ نوامبر ۱۹۸۸ ، روبرت موریس ، یکی از فارغ التحصیلان دانشگاه کورنل ایالات متحده ،کـرم رایانـه‌ای برنامـه‌ریـزی شده خود را در سطح گسترده‌ای از شبکه‌ای که در آن زمان آرپانت (Arpanet) نامیده می‌شد و بعدها نام اینترنت برخود گرفت، پخش کـرد. ایـن کـرم طی هشت ساعت، تقریباً سه هزار رایانه را با اختلال مواجه کرد. برای تعمیر این وضعیت، بسیاری از دسـتگاه‌هـای رایانـه‌ای از شـبکه جداشـد تـا بتـوان کپی‌های کرم مزبور رابه طور کامل حذف کرد. منبع پیشین، ص۷.

۵۴- SPAN

۵۵- Christmas Tree، ترکیبی از یک اسب تروا و نامه‌ای زنجیره ای (Chain Letter) است .این کرم اساساً به این منظور ایجاد شده بود که شبکه IBM را در روز کریسمس ۱۹۸۷ فلج کند.کرم مزبورکه با زبانی به نام Exec نوشته شده بود از کاربران می‌خواست عبارت "کریسمس" را بر روی صفحه نمایشگر خود تایپ کنند. سپس باتایپ کلمه مزبور درخت کریسمسی را بر روی صفحه نمایش نشان می‌داد و خود را به نام تمامی کاربران ذخیره شد در فایلهای Names و Netlog فرستاده و بدین ترتیب خود راتکثیر می‌کرد.

۵۶- Denial of Service

۵۷- Distributed Denial of Service

می‌شود.[۵۸] در واقع عمده علتی که سبب می‌شود این حملات پر خطر جلوه کنند، ماهیت محدود منابع سیستم و شبکه‌های رایانه‌ای همچون میزان پهنای باند، [۵۹] توان پردازش و قابلیت‌های ذخیره آنهاست.

برای مثال آنچه که سبب می‌شود یک ارائه کننده خدمات اینترنتی[۶۰] نتواند در برابر حجم داده بسیار بالایی که یک مهاجم تولید می‌کند و به کامپیوتر سرورهای آن ارائه کننده خدمات ارسال می‌کند، مقاومت نماید، در واقع میزان پایین حافظه ذخیره اطلاعات آن ارائه کننده خدمات نسبت به حجم داده‌های وارده است که سبب می‌شود کامپیوتر سرور ارائه کننده خدمات مختل شده و از کار بیفتد.

گاهی اوقات مهاجمین حملات DoS ، ا زطریق سیستم کاربران اقدام می‌کنند. برای مثال چنین کاربرانی با دیدن ترواهای موجود در سایت های اینترنت که به رایگان عرضه می‌شود، وسوسه می‌شوند که آنها را در کامپیوتر خود نصب و دوستان خود را اذیت کنند، غافل از اینکه ارائه کنندگان این ترواها، در واقع در صدد کشف و شناسایی سایر کاربرانی هستند که نامشان در لیست رایانه آن کاربران وجود دارد و بدین ترتیب با واسطه قراردادن آن کاربر و شناسایی سایرکاربران، حملات خود رانسبت به آنها به انجام می‌رسانند.[۶۱]

حملات DoS و DDoS امروزه از جمله حملات بسیار شایع برای ایجاد اختلال در کارکرد سیستم های رایانه‌ای هستند. اما چنانچه پیشتر نیز گفته شد، مهاجمین از سایر ابزارها نظیر ویروس‌ها، کرم‌ها و ترواهای رایانه‌ای نیز برای این منظور استفاده می‌کنند. برخی از شیوه‌های شایع حملات DoS عبارتند از:

قطره اشک (Teardrop) ، Syn floid, UDDF floiding، حملات زمینی (Land Attacks)، اشغال پهنای باند (Bandwidth Consumption)، اشغال سایر منابع (Consumption of other Resourses) و غرش مرگ (Ping of Death). [۶۲]

دیدگاه تطبیقی

از بین بردن و اختلال داده‌ها:

در غالب کشورها، مقررات مربوط به ایراد خسارت به اموال[۶۳] ، ناظر به تخریب اشیاء مادی و ملموس بوده و از این رو این مسأله که آیا از بین بردن و ایجاد اختلال در داده‌ها مشمول مقررات سنتی راجع به تخریب اموال می‌گردد یا نه، آن کشورها را با چالش حقوقی مواجه ساخته است.

۵۸- برای مثال در ژانویه ۲۰۰۲ ،بر اثر یکی از حملات اختلال در کارکرد سیستم ،ارائه کننده خدمات کلود ناین (Cloud Nine ISP) در انگلستان ، کاملاً از ارائه هرگونه خدمات رایانه‌ای بازماند.

۵۹- Bandwidth

۶۰- Internet Service Provider

۶۱- منبع پیشین ،همان ،ص۸

۶۲- منبع پیشین ،همان ،ص۸

۶۳- Damage to Property ،Destruction ،Vandalism ،Sabotage

معهذا غالباً کشورها به این نتیجه رسیده‌اند که برای از بین بردن و اختلال داده‌ها باید اقدام به وضع مقررات کیفری خاص گردد.

در مواد ۲۵۸ و ۲۵۹ کد کیفری بلژیک و نیز در مواد ۴۲۸ و ۴۳۰ کد کیفری کانادا، پاک کردن اطلاعات بدون ایراد خسارت فیزیکی نسبت به حامل آنها، تخریب اموال محسوب نشده و از اینرو مواد مزبور اختصاصاً برای از بین بردن داده‌های رایانه‌ای وضع شده‌اند.

معهذا غالباً کشورها به این نتیجه رسیده‌اند که برای از بین بردن و اختلال داده‌ها باید اقدام به وضع مقررات کیفری خاص گردد.

در کد کیفری کشورهای اتریش (ماده ۱۲۵)، دانمارک (ماده ۲۹۱) آلمان (ماده ۳۰۳)، ایتالیا (مواد ۴۲۰و ۶۳۵)، ژاپن (مواد ۲۵۸ تا ۲۶۱ کد کیفری و نیز مواد ۲۳۳ و ۲۳۴ قانون مربوط به اختلال در کسب وکار و تجارت)[۶۴]، هلند (ماده ۳۵۰)، نروژ (ماده ۲۹۱)، اسپانیا (مواد ۵۴۷ به بعد کد کیفری سابق) و سوئد (ماده ۲۱ از فصل دوازده کد کیفری)، صدمه عمدی که موجب تخریب اطلاعات بر روی دیسکت‌ها یانوارهای صوتی و تصویری می‌گردد را، ایراد خسارت به اموال دانسته‌اند. رویکرد مزبور بر این نظر مبتنی است که در این موارد باید بر ایراد خسارت فیزیکی نسبت به حاملهایی که اطلاعات در آنها ذخیره شده است تأکید گردد. لذا برای حل مسأله از بین بردن واختلال در داده‌هایی که مشمول مورد فوق نمی‌گردند، اتریش در بند الف ماده ۲۶۰، کانادا در فراز ۱ از بند ۱ ماده ۴۳۰، دانمارک درماده۱۹۳ کد کیفری (اصلاحی ۱۹۸۵)، آلمان در بند الف و ب ماده۳۰۳، فنلاند در مواد ۱تا۳ فصل ۳۵ کد کیفری اصلاحی ۱۹۹۰ و نیز در بند ۲ ماده ۱ فصل ۳۴ کد کیفری اصلاحی ۱۹۹۵، فرانسه در مواد ۴۶۲ تا ۴۶۴، هند در ماده ۶۶ قانون فناوری اطلاعات[۶۵] مصوب ۲۰۰۰ ،ژاپن در مواد ۲۳۲تا ۲۳۴ ونیز مواد ۲۵۸ و ۲۵۹ هلند در بند الف و ب ماده ۳۵۰، اسپانیا دربند ۲ ماده ۲۶۴، سوئد درماده ۲۱ قانون حمایت داده[۶۶]، سوئیس در ماده ۱۴۴، انگلستان در ماده۳ قانون سوء استفاده از رایانه[۶۷] و ایالات متحده در فراز پنجم از بند الف ماده۱۰۳۰ کد کیفری خویش، اقدام به وضع قواعدی کیفری در راستای ازبین بردن و ایجاد اختلال در داده‌ها نموده‌اند.[۶۸]

در سیستم حقوقی برخی از کشورها، برای مواردی که سبب می‌گردد با از بین بردن و اختلال داده‌ها امور تجاری یا امنیت ملی مختل شود، مجازات شدیدتری وضع شده است .

در این خصوص در سطح بین‌المللی نیز فعالیت‌هایی صورت گرفته که از آن جمله می‌توان به اقدامات OECD، کشورهای گروه ۸، اتحادیه و شورای اروپا اشاره کرد. کاملترین متن بین‌المللی که تاکنون درخصوص جرایم رایانه‌ای به تصویب رسیده، کنوانسیون بوداپست شورای اروپاست که برای هماهنگ‌سازی قوانین کشورهای عضو تنظیم شده و موضوع از بین بردن واختلال در داده‌ها طی ماده ۴ آن و با عنوان اختلال درداده‌ها[۶۹] پیش بینی شده است .

۶۴- Obstruction of Business Act
۶۵- Information Technology Act
۶۶- Data Protection Act
۶۷- Computer Misuse Act
۶۸- Cyber terrorism in the Context of Globalization، همان، صص۱۵ و ۱۶.
۶۹- Data Interference

طی بند ۱ ماده مزبور "هریک از اعضاء باید به گونه‌ای اقدام به وضع قوانین ومقررات نماید که در صورت لزوم بر اساس حقوق داخلی خود ، هرنوع صدمه زدن، پاک کردن،تخریب ،دستکاری یامتوقف کردن داده‌ها ی کامپیوتری راکه به طور عمدی ومن غیرحق صورت می‌گیرد جرم انگاری نماید.

در بند ۲ ماده فوق نیز آمده است که «عضو مورد نظر میتواندحق واکنش در برابر افعال مندرج در بند ۱ رادرصورتی که ضرر عمده‌ای وارد شده باشد، مقرر دارد».[۷۰]

اختلال در کارکرد سیستم رایانه‌ای:

ایجاد اختلال در کارکرد سیستم رایانه‌ای، در برخی کشورها مورد جرم انگاری قرار گرفته که ازآن جمله می‌توان به استرالیا (بند ج ماده ۷۶ قانون جرایم[۷۱] مصوب ۱۹۱۴)، کانادا (فراز ۱ از بند ماده۴۳۰ کد کیفری)، آلمان (بندب ماده ۳۰۳ کد کیفری)، هند (بند ز ماده ۴۳ قانون فناوری اطلاعات مصوب ۲۰۰۰) و سنگاپور (ماده ۷ قانون سوء استفاده از رایانه [۷۲]) اشاره کرد .[۷۳] این امر درماده ۵ کنوانسیون جرایم محیط سایبرشورای اروپا (بوداپست) نیز با عنوان اختلال درسیستم[۷۴] بیان شده است. طبق ماده مزبور: " هریک از اعضاء باید به گونه‌ای اقدام به وضع قوانین و مقررات نماید که در صورت لزوم، براساس حقوق داخلی خود، هرنوع ایجاد اختلال عمدی و بدون مجوز عمده‌ای راکه در کارکرد سیستم رایانه‌ای و در اثر واردکردن، انتقال، صدمه زدن، پاک کردن، ازبین بردن، دستکاری یا متوقف کردن داده‌های رایانه‌ای بوجود می‌آید، جرم انگاری کند."[۷۵]

تولید، توزیع و انتشار برنامه‌های مخرب:

برخی از کشورها در خصوص صرف انتشار و واردکردن برنامه‌های مخرب و مختل کننده در سیستم وشبکه‌های رایانه‌ای، صرفنظر از اینکه موجب تخریب واختلال در داده‌ها یا سیستم رایانه‌ای شود یاخیر، اقدام به وضع مقررات کیفری نموده‌اندکه از آن جمله می‌توان به ایتالیا (ماده ۶۱۴ کد کیفری) و هلند اشاره کرد. سوئیس یک مرحله پیش‌تر رفته و علاوه بر انتشار این‌گونه برنامه‌ها، تولید و آموزش تولید چنین برنامه‌هایی را نیز به طور مستقل جرم انگاری کرده است .

در هند ماده ۶۴ قانون فناوری اطلاعات مصوب ۲۰۰۰، به این امر اختصاص دارد. در ایالات متحده نیز شش ایالت کالیفرنیا، ایلینویز، مین، مینسوتا، نبراسکا و تگزاس در این خصوص اقدام به وضع قانون کیفری نموده‌اند.[۷۶]

معذالک کنوانسیون بوداپست شورای اروپا به امر تولید، انتشار، توزیع، معامله و ارائه این برنامه‌ها در خارج از محیط سیستم و شبکه رایانه‌ای اشاره کرده است. طبق ماده ۶ (بند الف) کنوانسیون مزبور:"هریک از اعضاء باید به گونه‌ای اقدام به وضع

۷۰- کنوانسیون جرایم محیط سایبر، بوداپست ۲۰۰۱، ترجمه امیرحسین جلالی، شورای عالی توسعه قضایی، ص۵.

۷۱- Crimes Act.

۷۲- Computer Misuse Act.

۷۳- Cyber Terrorism in the Context of Globalization. همان ،صص ۱۷و۱۸.

۷۴- System Interference

۷۵- کنوانسیون جرایم محیط سایبر، همان، ص ۵.

۷۶- Cyber Terrorism in the Context of Globalization. همان ،ص ۱۷.

قوانین و مقررات نماید که در صورت لزوم بر اساس حقوق داخلی خود، هرگونه اقدامات عمدی و بدون مجوز ذیل را جرم انگاری نماید:

الف) تولید، فروش، تأمین، وارد کردن، توزیع و یا به نحوی در دسترس گذاردن وسایلی که در بردارنده برنامه کامپیوتری است واساساً به منظور ارتکاب هر یک از جرایم مندرج در مواد ۲ تا۵ طراحی شده است..."

در بند ب ماده مزبور نیز پیشنهاد شده که حتی در اختیار داشتن برنامه‌های مخرب و مختل کننده توسط دولت‌های عضو جرم انگاری گردد.[۷۷] (چنانچه قبلاً بیان گردید مواد ۴و۵ کنوانسیون مزبور به اختلال در داده‌ها و کارکرد سیستم‌های رایانه‌ای اختصاص دارد.)

نتیجه‌گیری:

سیر تحول جوامع امروز شدیداً با وجود سیستم‌ها و داده‌های رایانه‌ای گره خورده است. این وابستگی، از سویی موجب تسهیل روند فعالیت‌های اجتماعی و اقتصادی گشته، و از سوی دیگر برای بزهکاران فرصتی ایجاد کرده که بتوانند بواسطه از بین بردن، اختلال و غیرقابل استفاده کردن داده‌ها یا اختلال در کارکرد سیستم‌های رایانه‌ای، امنیت داده‌ها و شبکه‌های رایانه‌ای را به خطر افکنده و بدین ترتیب به مقاصد شوم خویش نائل آیند.

تدوین قوانین کیفری در راستای مبارزه با این فرایند در کنار سایر ابزارهای حقوقی- اجتماعی کنترل این جرایم، می‌تواند حربه‌ای مؤثر برای مقابله با این پدیده به غایت خطرناک باشد. قوانین سنتی کشورها در این زمینه، غالباً ساکت و یا ناکافی است. بدین‌ترتیب کشورها و علی‌الخصوص کشورهایی که میزان وابستگی اجتماعی- اقتصادی آنها به محیط سایبر بیشتر است، اقدام به اصلاح یا وضع قوانین کیفری در این زمینه کرده‌اند. احساس این وابستگی به محیط سایبر، در کشور ما نیز هر روز افزونتر می‌گردد و بدین ترتیب باید بر آن بود که مقنن ایران نیز باید در راستای حمایت از امنیت داده‌ها و سیستم‌های رایانه‌ای کاربران، دستگاه‌های دولتی، نهادهای عمومی و مؤسسات خصوصی اقدام به وضع قوانین کیفری یا اصلاح قوانین موجود نماید تا بدین ترتیب موجبات امنیت داده‌ها و شبکه‌های رایانه‌ای و در نتیجه رشد و توسعه اجتماعی و اقتصادی کشور را در محیط سایبر فراهم آورد.

۷۷- کنوانسیون جرایم محیط سایبر، همان صص ۵و۶.

منابع و مأخذ

منابع فارسی:

۱- فرهنگ تشریحی کامپیوتر، مایکروسافت، ۲۰۰۳، ترجمه: دکتر رضا حسنوی و مهندس داریوش فرسایی، ویرایش پنجم، انتشارات دانشیار، ۱۳۸۱.

۲- کنوانسیون جرایم محیط سایبر، بوداپست ۲۰۰۱، ترجمه امیرحسین جلالی، شورای عالی توسعه قضایی.

منابع لاتین:

1- computer Crime abuse Report (India) 2001-2002www.asianlaws.org/report0102.pdf
2- CRS Report Congres, Cyber Warfare, updated march 2003
http://fpc.state. gov/documents/organization/19134.pdf
3- Cyber Laws: A Perspective
http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN005846.pdf
4- Cyber Terrorism in the context of Globalization- www.ieid.org/congreso/ponencias/Nagpal, Rohas.pdf
5- How to Prevent Cyber Sabotage
www.giac.org/practical/GSEC/James_harris_GSEC.pdf
6-Protecting IT Systems from Cyber Crimes
www.cs.ncl.ac.uk/Research/Pubs/articles/paper/311.pdf
7- Webpage Defacement Cuntermeasures
www.Scit.wiv.ac.uk/in 8189/pdf

☑ **عنوان: صلاحیت قضایی در محیط مجازی**

☑ **نویسنده: شاهپور دولتشاهی** (کارشناس ارشد حقوق جزا و جرم شناسی)

بخش اول ـ صلاحیت در آیین دادرسی کیفری

مقدمه

صلاحیت کیفری را می‌توان به توانایی و شایستگی قانونی و نیز تکلیف مرجع قضایی، به رسیدگی به یک دعوای کیفری تعبیر کرد. بنابراین نخستین مسأله‌ای که مراجع تحقیق باید به آن بپردازند، بررسی صلاحیت خود جهت شروع به تحقیقات است و در صورتی که خود را صالح به رسیدگی ندانند موظف به اصدار قرار عدم صلاحیتند. ماده ۳۲ قانون تشکیل دادگاههای عمومی و انقلاب، تشخیص صلاحیت را عهدهٔ همان دادگاه رسیدگی کننده نهاده است.

این ماده مقرر می‌دارد: «تشخیص صلاحیت یا عدم صلاحیت هر دادگاه نسبت به دعوای مطروحه با همان دادگاهی است که قانوناً مکلف به رسیدگی به پرونده بوده است».

ماده ۳۳ قانون مذکور می‌افزاید: «در صورتی که دادگاه رسیدگی کننده، خود را صلاح به رسیدگی نداند با صدور قرار عدم صلاحیت، پرونده را به دادگاه صالح ارسال می‌نماید ...».

برخی از ویژگی‌های صلاحیت کیفری عبارتند از:

۱ـ صلاحیت ناظر به نظم عمومیست.

منظور این است که مقررات مربوط به صلاحیت، در جهت اعمال صحیح‌تر عدالت قضایی وضع شده است و به همین دلیل، و برخلاف امور حقوقی که در پاره‌ای از موارد اصحاب دعوا می‌توانند با توافق یکدیگر از صلاحیت مرجع خاص عدول کنند، در امور کیفری عدم رعایت قواعد و مقررات راجع‌به صلاحیت، حتی با توافق یکدیگر، تجویز نشده است و نادیده گرفتن این قواعد، جز در موارد استثنایی مصرح در قانون، نقض حکم یا قرار صادره از سوی مراجع تالی، توسط دادگاه‌های عالی را در بردارد.

۲ ـ تکلیف مراجع قضائی در خصوص رسیدگی به صلاحیت خود.

کلیه مراجع کیفری مکلفند، قبل از شروع به تحقیق و رسیدگی، بدقت صلاحیت خود را بررسی کنند.

به عبارت دیگر، خود مرجع رسیدگی کننده باید صرف نظر از ایراد اصحاب دعوا (دادستان، شاکی و یا متهم) صالح بودن خود جهت رسیدگی را احراز کند و در صورت لزوم به اصدار قرار عدم صلاحیت مبادرت ورزد. به طریق او لی، آنگاه که صلاحیت از سوی یکی از اصحاب دعوا مورد تردید قرار گیرد مسأله احراز آن با دقت بیشتری مورد توجه قرار گیرد.

۳ – قبول ایراد عدم صلاحیت در کلیه مراحل رسیدگی.

ایراد عدم صلاحیت اختصاص به مرحله بدوی رسیدگی ندارد و در تمام مراحل رسیدگی اعم از بدوی، استیناف و فرجام قابل اعلام است.

نکته دیگر اینکه، از دیدگاه حقوقی، حاکمیت دولتها به مرزهای زمینی، دریایی و هوایی آنها محدود می‌شود و درنتیجه اعمال حاکمیت کیفری یعنی تعقیب و به کیفر رسانیدن بزهکاران اصولاً نباید نسبت به جرائم ارتکابی خارج از محدوده مرزها تسری یابد. تخطی از این اصل، مستقیماً بمنجر به تجاوز به قلمرو حاکمیت دیگر کشورها خواهد شد. در این موقعیت، رعایت اصل صلاحیت درون مرزی، مطرح می گردد و در این خصوص، تعیین صلاحیت مراجع کیفری داخلی واجد اهمیت بسیار است.

وقتی جرمی اتفاق افتاد، به کمک قواعد مربوط به صلاحیت می‌توان دریافت که در بین کلیه مراجع کیفری موجود در کشور کدام یک باید نسبت به تحقیق از متهم و محاکمه و مجازات او اقدام کنند. برای مثال وقتی اتهام خیانت به میهن و جاسوسی به شخصی نسبت داده شد باید دید کدام یک از دادگاهها، اعم از عمومی و اختصاصی، شایستگی رسیدگی به آن را دارد (صلاحیت ذاتی). چنانچه جرمی در صلاحیت دادگاههای عمومی یا دادگاههای اختصاصی، مثلاً دادگاه انقلاب باشد، باز هم باید مشخص گردد که دادگاه عمومی یا انقلاب کدام نقطه از کشور باید اقدام کند (صلاحیت محلی). سرانجام برخی ویژگی‌های شخصی مرتکب اعم از موقعیت، سن، شغل و مسئولیت ممکن است موجب رسیدگی مرجع خاصی شود (صلاحیت شخصی). اما قبل از بررسی این امر که کدام دادگاه ایرانی صالح به رسیدگی است باید مشخص شود که اصولاً رسیدگی به جرم ارتکابی در صلاحیت مراجع کیفری ایران قرار دارد یا این امر باید توسط یک مرجع خارجی صورت پذیرد و یا چون قبلاً توسط یک مرجع خارجی مورد رسیدگی قرار گرفته است دیگر قابل طرح در محاکم داخلی نیست.

مبحث اول: صلاحیت برون مرزی در قانون مجازات اسلامی

در موارد ذیل، چنانچه حتی جرم در خارج از قلمرو حاکمیت زمینی، هوایی و دریایی جمهوری اسلامی ایران اتفاق بیافتد، مراجع کیفری ایران صلاحیت رسیدگی دارند:

۱) در مورد ایرانیانی که در خارج از کشور مرتکب جرم می شوند، اعم از اینکه بزه ارتکابی از بزه‌های مندرج در ماده ۵ قانون مجازات اسلامی یا هر جرم دیگری باشد (ماده ۷ قانون مذکور)، صلاحیت رسیدگی به مراجع داخلی واگذار شده است.

قانونگذار با استعمال عبارت «هر ایرانی که در خارج ایران مرتکب جرمی شود ....» در ماده ۷ قانون مجازات اسلامی، تفاوتی بین کارمندان دولت و سایرین و نیز نوع جرم ارتکابی قائل نشده است.

در مواردی که قسمتی از جرم در ایران ارتکاب یابد ولی نتیجه آن در خارج حاصل شود و برعکس نیز، به طریق او لی، صلاحیت رسیدگی با دادگاههای داخلی است (ماده ۴ ق.م.ا).

۲) در مورد جرائم بین‌المللی از قبیل قاچاق مواد مخدر، تروریسم، بچه‌دزدی، معامله فحشا و هواپیماربایی که طبق قانون خاص یا عهود بین‌المللی مرتکب در هر کشوری یافت شود، در همان کشور محاکمه می‌گردد، چنانچه متهم در ایران دستگیر شود دادگاههای ایرانی صلاحیت رسیدگی داشته و متهم طبق قانون مجازات اسلامی به کیفر خواهد رسید (ماده ۸ ق.م.ا).

مبحث دوم: صلاحیت درون مرزی مراجع کیفری

همه دادگاه‌ها و مراجع تحقیق موجود در کشور، صالح به رسیدگی به همهٔ جرائمی که در سطح کشور یا در حوزهٔ قضایی آنها اتفاق می‌افتد نیستند. به عبارت دیگر رسیدگی به جرائم، باید بین مراجع رسیدگی تقسیم شود و هر یک از آنها شایستگی و توانمندی رسیدگی به تعدادی از جرائم یا جرائم با ویژگی‌های خاص، بویژه با توجه به نوع اتهام، را دارند. بدین ترتیب، پس از وقوع و کشف جرم، این پرسش اساسی و مهم مطرح می‌شود که تعقیب متهم، انجام دادن تحقیقات مقدماتی و سرانجام محاکمه و رسیدگی توسط کدام یک از مراجع کیفری موجود در کشور باید انجام شود. پاسخ به این پرسش را باید در قواعد حاکم بر صلاحیت مراجع کیفری داخلی، جستجو کرد.

مبحث سوم، صلاحیت محلی در قانون آئین دادرسی کیفری

قانون آیین دادرسی دادگاه‌های عمومی و انقلاب در امور کیفری در مبحث سوم از فصل دوم (ماده ۵۱) پس از تذکر این مطلب که دادگاه‌ها فقط در حوزهٔ قضایی محل مأموریت خود ایفای وظیفه می‌کنند و به عبارت دیگر با تحدید اختیار رسیدگی دادگاه‌ها به حوزهٔ قضایی محل مأموریت، جهات قانونی برای شروع به تحقیق و رسیدگی را به شرح زیر بیان داشته است:

۱) جرم در حوزهٔ قضایی آن دادگاه واقع شده باشد.

۲) جرم در حوزهٔ قضایی دیگری واقع شده ولی در حوزهٔ قضایی آن دادگاه کشف یا متهم در آن حوزه دستگیر شده باشد.

۳) جرم در حوزه دادگاه دیگری واقع ولی متهم یا مظنون به ارتکاب جرم در حوزهٔ آن دادگاه مقیم باشد.

بدین ترتیب، مقنن ایرانی در قانون آیین دادرسی کیفری جدید (همانند قانون آیین دادرسی کیفری ۱۲۹۰ شمسی) ضوابط چهارگانهٔ محل وقوع، محل کشف، اقامتگاه و محل دستگیری را در تعیین صلاحیت محلی مراجع کیفری عمومی و انقلاب مد نظر داشته. النهایه حق تقدم برای محل وقوع جرم قائل شده است و در مادهٔ ۵۴ مقرر می‌دارد: «متهم در دادگاهی محاکمه می‌شود که جرم در حوزهٔ آن واقع شده است...» . بدین ترتیب در مواردی که جرمی خارج از حوزه قضایی دادگاه واقع شده لیکن در حوزه آن کشف یا مرتکب در حوزهٔ آن دستگیر شود و نیز در مواردی که دادگاه صلاحیت محلی برای رسیدگی نداشته باشد دادگاه موظف است تحقیقات مقتضی و ضروری را به عمل آورده و پرونده را همراه با متهم (در صورت دستگیری) به دادگاه محل وقوع جرم ارسال دارد.

توجه قانونگذار و تأکید رویه قضایی بر صلاحیت مرجع کیفری محل وقوع جرم سبب می‌شود که دادگاه حوزه اقامت متهم را نیز مکلف به ارسال تحقیقات انجام شده نزد دادگاه محل وقوع جرم بدانیم. بدیهی است در مواردی که محل وقوع جرم مشخص نباشد دادسرای محل کشف مکلف است به تحقیقاتی که شروع کرده تداوم بخشد تا وقتی که تحقیقات ختم یا محل وقوع جرم معلوم شود. چنانچه محل وقوع جرم مشخص نگردد تعقیب را ادامه داده و سپس دادگاه اقدام به صدور رأی می‌کند.

با این همه باید گفت که پس از محل وقوع جرم، محل دستگیری متهم در حقوق ایران و در مرحله دوم در تعیین صلاحیت مؤثر است. برای مثال، چنانچه جرائم ارتکابی از حیث مجازات از یک درجه باشد طبق ماده ۵۴ قانون آیین دادرسی دادگاه‌های عمومی و انقلاب در امور کیفری، دادگاهی که مرتکب در حوزهٔ آن دستگیر شده صالح به رسیدگی خواهد بود. توضیح اینکه متهم ممکن است مرتکب چند جرم در حوزه‌های قضایی مختلف شود در این صورت بصراحت صدر مادهٔ ۵۴ قانون مذکور، در دادگاه‌هایی که مهمترین جرم در حوزهٔ آن واقع شده است محاکمه خواهد شد. لیکن چنانچه جرائم ارتکابی از حیث مجازات در

یک درجه باشد ، دادگاه محل دستگیری صلاحیت رسیدگی خواهد داشت. در این صورت چنانچه اقدامات تحقیقی به وسیله سایر دادگاه‌ها(ی محل وقوع جرائم دیگر)، بعمل آمده باشد، پرونده‌های متشکله به دادگاه محل دستگیری متهم ارسال خواهد شد. همچنین، در موردی که یکی از اتباع ایران در خارج از قلمرو حاکمیت جمهوری اسلامی ایران مرتکب جرمی شود، در صورت دستگیری در داخل کشور، در دادگاهی که در حوزهٔ آن دستگیری به عمل آمده است باید مورد محاکمه قرا ر گیرد.

در پایان یادآور می‌شویم در مواردی که جرائم منتسب به متهم در حوزه‌های قضای مختلف ارتکاب یافته ولی متهم دستگیر نشده باشد، دادگاهی که ابتدائاً شروع به تعقیب نموده، صلاحیت رسیدگی به کلیهٔ جرایم ارتکابی از ناحیه متهم را خواهد داشت.

برغم اهمیتی که صلاحیت محلی در رسیدگی به امور کیفری داراست، قانونگذار، خود در مواردی از قواعد عمومی ناظر به تعیین صلاحیت عدول نموده و صلاحیت موازی، برای مراجع متعدد رسیدگی در نظر می‌گیرد (مستثنیات) و یا تشخیص ضرورت عدم رعایت مقررات ناظر به صلاحیت محلی را، طی شرایطی، به مقامات قضایی واگذار می‌نماید. (احا له).

بخش دوم: چالشهای قواعد دادرسی سنتی در فضای سایبر

مقدمه

۱. همچنانکه انسان به سدهٔ ۲۱ پای می‌گذارد، سخنان رهبر بومیان آمریکایی سدهٔ نوزدهم، کوشیس، به ناگاه معنایی تازه می‌یابند. او که رئیس قبیله آپاچ بود و در سال‌های آخر عمر خود در حصارهای ناپیدای یک اردوگاه دولتی برای سرخپوستان گرفتار آمده بود، به خوبی از نقش محوری مرزهای جغرافیایی در احکام حقوقی غرب آگاه بود. ولی حتی او هم نمی‌توانست پیش‌بینی کند که پیش از به پایان رسیدن هزارهٔ دوم، فن‌آوری سفیدپوستان، با سرعت و شدتی بیشتر از عناصر طبیعی، این خطوط تخیلی را خواهد زدود.

۲. بویژه، گسترش شبکه‌های جهانی رایانه‌ای چندیست که مرزهای جغرافیایی را با خلل روبه رو کرده است. استفاده از شبکه‌های جهانی اینترنتی به شدت رو به افزایش است. همین که پیوستن به شبکه‌های اینترنتی افزایش می‌یابد ـ یعنی جایی که بسیاری از از افراد با هم تبادل دارند ـ مباحث حقوقی، اهم از کیفری و خصوصی به شکل تازه‌ای مطرح می‌گردد.

مبحث اول – نامعین بودن حیطه‌های جغرافیایی

قوانین و مقررات حاکم بر بستر عبور و مرور در فضای مبادلات اینترنتی بی شک، از مقررات موجود برای مبادلات تجاری در دنیای واقعی، بسیار متفاوت خواهند بود. بخش عمده‌ای از این تفاوت ناشی از خصوصیاتی است که در اینترنت، زمینهٔ حضور راه دور را فراهم می‌آورند و شبکه را به لحاظ فن‌آوری از بُعد مکانی و فیزیکی متمایز می‌کنند. موقعیت شبکه آنچنان به موقعیت جغرافیایی بی‌ربط است که اغلب تعیین مکان فیزیکی یک منبع یا کاربر اینترنتی ناممکن است. اطلاع از این موقعیت مکانی برای عملکرد شبکه و ایجاد کنندگان آن اهمیتی ندارد، لذا در طراحی یک شبکه امکان تشخیص مکان جغرافیایی در نظر گرفته نشده.

در فضا و مکان واقعی، یک شرکت یا طرف تجاری معمولاً می‌تواند مکانی واحد یا شخصی را که با او در تبادل است شناسایی نماید. چرا که این کار به شناسایی طرفین و اعتبار و مشروعیت مبادلات کمک می‌کند. ولی انجام این کار در محیط مجازی

رایانه‌ای بسیار دشوار است. زیرا در اینجا طرفین یک مبادله ممکن است در دو اتاق هم جوار یا در دو سوی جهان باشند و شبکه هم راهی برای تشخیص این تفاوت ارائه نمی‌دهد. ماشین‌های اینترنتی «آدرس» دارند ولی این آدرس جایگاه آنها را در شبکه مشخص می‌کند نه در مکان و موقعیت ارضی. البته بعضی آدرس‌های اینترنتی مشخص‌کننده‌های جغرافیایی، یا مشخص‌کننده‌هایی که از نظر جغرافیایی قابل تعیین باشند را در خود دارند. برای مثال، یک آدرس اینترنتی که پسوند (UK) را داشته باشد در بریتانیای کبیر(United Kingdom) قرار دارد.

ولی متأسفانه اکثر آدرس‌های اینترنتی فاقد چنین تعیین‌کننده‌های جغرافیایی هستند. مهمتر از آن، تمام آدرس‌های اینترنتی به راحتی قابل انتقال هستند، زیرا برخلاف آدرس‌های فیزیکی در فضای واقعی زندگی آدرس‌هایی قراردادی در شبکه هستند. به عبارت دیگر، هیچ‌گونه هماهنگی و هم‌سویی بین فضا و مکان واقعی از یک سو و فضای مجازی رایانه‌ای وجود ندارد.

مبحث دوم – صلاحیت قضایی در قبال مجرمین

مسائل مربوط به صلاحیت قضایی در قبال جرائم ، تقریباً همیشه با در نظر گرفتن محل ارتکاب آنها بیان می‌شوند. این بدان دلیل است که صلاحیت قضایی جنایی همواره بر مبنای حضور واقعی و فیزیکی مجرم در درون حوزهٔ استحفاظی و در مقابل میز محاکمه تعیین می‌شود. براساس قواعد صلاحیت قضایی اگر عنصر مادی یک جرم درون حوزهٔ قضایی شروع یا کامل شده باشد، آن حوزه قضائی صالح برسیدگی خواهد بود. در مورد جرائم چند صلاحیتی، مانند آدم‌ربایی، تنها کافی است که یک عنصر مادی از جرم، درون یک حوزه قضائی در حال انجام باشد تا آن حوزه صا لح برسیدگی شناخته شود.

تعامل و ادغام این قوانین ممکن است کاربران اینترنتی را با احتمال مجرم بودن در هر حوزه ذیصلاحی که با اینترنت در ارتباط است روبرو کند. همچنین ماهیت اینترنت امکان ارتباط متقابل بین چندین حوزهٔ قضایی را فراهم آورده و عناصر یک جرم ممکن است نه تنها در مکان و حوزه‌ای با حضور فیزیکی مجرم شروع شده، و یا به نتیجه رسیده باشند، بلکه این امکان نیز هست که در تمام حوزه‌های دیگری که در اثر عملکرد کاربر به صورت الکترونیکی درگیر شده‌اند نیز بحث وقوع جرم مطرح باشد.

اما مسئله مهم اینجاست که با توجه به ماهیت جرایم اینترنتی تعیین محل وقوع جرم و یا محل حصول نتیجه همیشه و به آسانی مقدور نیست و به فرض شناسایی محل ارتکاب جرم و یا محل حصول نتیجهٔ جرم (در صورت تعدد محلهای ارتکاب)، کدام حوزه صالح به رسیدگی خواهد بود و اگر چندین کشور درگیر چنین جرایمی شده باشند، اینکه کدام کشور و مهمتر اینکه داخل هر کشور، کدام‌یک از حوزه‌های قضایی داخلی، صالح به رسیدگی خواهند بود، موضوع بحث‌است!

اینک مطالعه‌ای تطبیقی در خصوص روشهای اتخاذ شده توسط برخی از کشورهای دنیا در قبال مسئله صلاحیت قضائی در رسیدگی به جرایم سایبر خواهیم داشت:

الف) **ایالات متحده**:

کشور ایالات متحده امریکا با توجه به اینکه متأثر از قواعد و قوانین کامن لا است، بیش از هر منبع و مأخذ حقوق نوشته، به عرف و رویه‌های قضایی استناد نموده و خصوصاً در استناد به قواعد عرفی، بیش از هر چیز مسئله انصاف و منطق را مدنظر قرار خواهد داد. در دادگاه‌های جنایی استنباط از عرف، عدل و انصاف و به معنای کلی، احراز نظر وجدان عمومی، بعهدهٔ هیأت منصفه نهاده شده.

در خصوص جرائم سایبر نیز، دادگاهها به عرف و منطق متوسل شده و در احراز و یا عدم احراز صلاحیت دادگاه، به ارتباط منطقی و عرفی میان کاربران اینترنتی و مجرمین اینترنتی توجه می‌نمایند. چرا که بدرستی دریافته‌اند چنانچه بخواهند با قواعد دادرسی کیفری سنتی به جرایم سایبر نیز رسیدگی کنند، می‌بایست به دنبال محل وقوع جرم، محل حصول نتیجهٔ مجرمانه و محل دستگیری متهم و ... گشت و با توجه به توضیحات قبلی در خصوص معین نبودن هیچیک از این مکانها در فضای مجازی، درگیر دور باطل خواهند شد. بنابراین از عرف، منطق و وجدان عمومی استمداد جسته و بحث «ارتباط منطقی» را مطرح نموده‌اند.

در بحث «ارتباط منطقی» ، دادگاه بررسی می‌کند که آیا متهم در جرائم سایبر، تا چه میزان موفق به برقراری ارتباط اینترنتی با بزهدیده گردیده و آیا این میزان برقراری ارتباط کافیست تا [دادگاه محل اقامت یا شکایت بزهدیده] صالح برسیدگی به اتهام مزبور باشد یا خیر! مثلاً اگر در ایالت کالیفرنیا صدها شهروند کالیفرنیایی در اثر ارتباط با یک وب سایت و مانورهای متقلبانه گردانندگان آن سایت اقدام به واریز مقادیر قابل توجهی پول به حسابهای مصرفی شده در سایت نموده و قربانی جرم کلاهبرداری شده باشند، چنانچه دادگاه تا این حد برقراری ارتباط میان سایت مذکور و کاربران (مالباخته) را از نظر منطقی مبنای رسیدگی خود قرار دهد، خود را صالح به رسیدگی به اتهام کلاهبرداری علیه شهروندان مالباختهٔ کالیفرنیایی دانسته و شروع به رسیدگی خواهد نمود.

اما در مقابل، چنانچه شهروندان کالیفرنیایی بدون توجه به تبلیغات فریبندهٔ وب سایت مزبور، و یا علیرغم تمام تلاش مدیران سایت جهت جلب نظر مخاطبان خود، ارتباط قابل توجهی با این سایت برقرار ننمایند، دادگاه به این نتیجه خواهد رسید که عدم برقراری ارتباط میان سایت و مخاطبان (شهروندان کالیفرنیایی) و یا حتی اندک ارتباط میان آنها، به حدی نیست تا بتوان بر مبنای آن، دادگاه کالیفرنیا را حائز صلاحیت و درگیر رسیدگی قضایی نمود.

تشخیص این امر که ارتباط پدید آمده در چه حد از اهمیت است و این حد ارتباط برای احراز صلاحیت دادگاه محل اقامت بزهدیدگان کافیست یا خیر، بعهده خود دادگاه است و ملاک و معیار این تشخیص، عرف، منطق و رجوع به رویه قضائی خواهد بود و این امریست که فقط در سیستم حقوقی کامن لا و در کشورهایی از جمله ایالات متحده قابل اجراست چرا که در کشورهای دارای سیستم حقوق نوشته، احراز صلاحیت دادگاه نه براساس رجوع به عرف و منطق حقوقی بلکه با توجه به نصوص صریح قانونی از پیش نوشته، صورت می‌پذیرد.

ب) کشورهای اروپایی (حقوق نوشته):

اغلب کشورهای اروپایی از جمله، فرانسه، بلژیک، آلمان و ... دارای رژیم حقوقی نوشته هستند.

قبل از وارد شدن به بحث صلاحیت قضایی در کشورهای دارای حقوق نوشته یادآور می‌شویم قریب به اتفاق کشورهای پیشرفته(حدود ۴۰ کشور)، با عضویت در کنوانسیون بین المللیِ جرایم محیط سایبر، تحت عنوان کنوانسیون بوداپست ـ۲۰۰۱، سیستم واحدی را که کنوانسیون در خصوص کلیات، تعاریف، جرایم، مجازاتها و دادرسی کیفری جرایم محیط سایبر پیشنهاد نموده، بطور متحد پذیرفته‌اند.

ج) کنوانسیون جرایم محیط سایبر ـ بوداپست ۲۰۰۱

بخش دوم از فصل دوم کنوانسیون، تحت عنوان صلاحیت، به تبیین اصول کلی صلاحیت کشورهای عضو در رسیدگی به جرایم محیط مجازی پرداخته.

در این بخش تنها یک ماده (ماده ۲۲) دارای ۵ بند، به این مهم اختصاص یافته. هر چند نقد ماده ۲۲ کنوانسیون، در حوصله این مقال نمی‌گنجد، اما بناچار و به نحو گذرا به بررسی این ماده می‌پردازیم:

بند ۱:

«هر یک از اعضاء باید به گونه‌ای اقدام به وضع قوانین و مقررات بنماید که در صورت لزوم در زمانی که جرم در موارد ذیل به وقوع می‌پیوندد، صلاحیت رسیدگی به هر یک از جرایم مندرج در مواد ۲ تا ۱۱ کنوانسیون را بوجود آورد:

الف) جرم در قلمروش بوقوع پیوسته باشد. یا:

ب) جرم در کشتی‌ای بوقوع پیوسته که پرچم آن کشور بر فراز آن برافراشته باشد. یا

ج) جرم در هواپیمایی بوقوع پیوسته که مطابق مقررات آن عضو به ثبت رسیده. یا:

د) در جایی که جرم مورد نظر مطابق قوانین جزایی قابل مجازات شناخته شده و توسط تبعه‌اش ارتکاب یافته یا جرم ارتکابی از جمله جرایم واقع در حوزه صلاحیت جهانی حقوق جزا باشد.»

صدر بند ۱ ماده ۲۲ بگونه‌ای نگارش یافته که این امید را زنده می‌کند: که کشورهای عضو مجاز شناخته شده‌اند تا قوانین خاص و جدیدی در راستای پیشگیری و مبارزه با جرایم محیط سایبر و منطبق با ماهیت مجازی شبکه، وضع نمایند. اما بلافاصله با برشمردن شقوق ۴ گانه، این گمان را از ذهن بیرون می‌برد و وضع به حالت دادرسی‌های سنتی برمی‌گردد.

شقوق چهارگانهٔ بند ۱ ماده ۲۲ دقیقاً همان مواردی را دربرمی‌گیرد که در دادرسی‌های کیفری سنتی خوانده‌ایم. حال آنکه ورود آنها در قوانین محیط سایبر نه تنها هیچگونه انطباقی با اوضاع و احوال و شرایط ارتکاب جرایم سایبر ندارد بلکه با آن منافات نیز دارد.

مثلاً در خصوص کشتی صاحب پرچم و یا هواپیما، فرض ارتکاب جرم سایبر، بسیار نادر و حتی در بسیاری موارد غیر ممکن بنظر می‌رسد. حتی اگر عقیده داشته باشیم که: «فرض محال، محال نیست» ، باز هم این ماده بسیار ناقص بنظر می‌رسد چون زمانیکه ما درگیر بحث تعیین صلاحیت سرزمینی کشورها در جرایم سایبر هستیم، بحث از جرایم ارتکابی در کشتی و هواپیما، لغو و بیهوده است چرا که این موارد (کشتی، هواپیما و ...) تحت شرایط خاص خود، جزئی از قلمرو حاکمیت کشور صاحب پرچم به حساب آمده و ابهام و اجمالی در صلاحیت کشور صاحب پرچم در مورد رسیدگی به جرایم ارتکابی در این گونه ادوات وجود ندارد و فرقی نیست میان جرایم سنتی مثل قتل و یا ضرب و جرح و ... و جرایم سایبری ارتکاب یافته در کشتی و هواپیما.

در خصوص جرایم ارتکابی توسط تبعه و یا جرایم حوزه صلاحیت جهانی، در قوانین دادرسی سنتی هیچ‌یک از کشورها ابهامی در صالح بودن کشور صاحب قلمرو نیست و اصلاً نیازی به دوباره نویسی این موارد در بند ۱ نبوده.

بحث اصلی، حل این مسئله است که در جرایم سایبر، اصلاً محل وقوع جرم کجاست ؟! و مجرم کیست ؟!

زمانیکه این سؤا لات پاسخ داده نشده چگونه می‌توان به تبیین صلاحیت سرزمینی و یا شخصی برای کشورها پرداخت ؟ آیا ابتدا نباید دانست جرم در حوزه کدام کشور و توسط چه شخصی ارتکاب یافته و بعد، حوزهٔ ارتکابی را صالح برسیدگی دانست ؟!

بند ۲ ماده ۲۲ نیز، چون ناظر به شقوق ب تا د بند ۱ است، تبعاً با سؤالات فوق روبروست.

بند ۲:

«هر یک از اعضاء می‌توانند حق عدم اجرا یا اجرای موضوعات یا شرایط بخصوصی را در محدوده مقررات صلاحیتی مندرج در شقوق ب تا د این ماده یا قسمتی از آن برای خود محفوظ دارند.»

به صراحت قسمت دوم بند ۳ ماده ۲، این قواعد صلاحیتی را در جایی مجری دانسته که متهم در حوزه کشور عضو قرار دارد و کشور عضو آن متهم را با استناد به اصل عدم استرداد تبعه، به کشور تقاضا کنندهٔ استرداد، مسترد نمی‌دارد. پس کشور عضوی که متهم در آن قرار دارد را ملزم به احراز صلاحیت کیفری خود و محاکمه و مجازات مرتکب نموده.

بند ۳:

«هر یک از اعضاء باید به گونه‌ای اقدام به وضع قوانین و مقررات نماید که در صورت لزوم امکان وضع صلاحیت در باره جرایم مندرج در پاراگراف ۱ ماده ۲۴ این کنوانسیون وجود داشته باشد. این موارد در جایی است که متهم در قلمرو آن عضو قرار دارد و آن عضو نیز متهم مورد نظر را صرفاً به خاطر تابعیت و پس از دریافت درخواست استرداد از طرف دیگر دولت عضو، مسترد نمی‌کند».

در بند ۴ ماده ۲۲ ,کنوانسیون را معارض قوانین صلاحیت داخلی کشورها ندانسته و به نوعی خواسته تاکشورها را ترغیب به وضع قواعد صلاحیتی در این باب نماید.

بند ۴:

« این کنوانسیون مانع اجرای هرگونه صلاحیت کیفری که مطابق قانون داخلی به مرحله اجرا درمی‌آید نمی شود. »

همانطور که ملاحظه میشود بازهم کنوانسیون راه حل عملی و منطقی در راستای حل معضلات صلاحیت ارائه نمی‌کند . ازسوی دیگر بدیهی است که کشورهای عضو در هرکنوانسیون, اختیارات داخلی قانونگذاری خود در مسایل مختلف حقوقی , خصوصاً حوزه قانونگذاری حقوق کیفری را ساقط و یا محدود نمی‌کنند وتصریح بند ۴ به این اختیار دولتها ,امری راهگشا نخواهد بود .

دربند ۵ ماده ۲۲ بحث تعارض صلاحیت دولتها در جائیکه چند کشور صالح به رسیدگی هستند مطرح گردیده اما تنهاراه حلی که ارائه شده به شور نشستن کشورهای صالح و انتخاب یک کشور و تفویض اختیار تعقیب و رسیدگی قضایی به کشور منتخب بوده است. چنانچه گذشت ، حتی بند ۵ نیز راه حلی در جهت حل تعارض صلاحیتها ارائه نداده و تنها شور وانتخاب نماینده رابرای رسیدگی کیفری پیشنهاد نموده.

مسائل لاینحل:

اول : تعیین محل ارتکاب جرم سایبر

دوم: شناسائی تابعیت شخص مرتکب

سوم: حل تعارض صلاحیت‌ها

مسئله اول ـ تعیین محل ارتکاب جرم سایبر :

جرم سایبر بلحاظ ماهیت مجازی وغیر واقعی خود, حقیقتاً نمود عینی و ملموسی، شبیه آنچه در جرایم سنتی مثل ضرب وجرح و یاسرقت و ... مشاهده می‌کنیم از خود به نمایش نمی‌گذارد . بلکه جرم سایبر در واقع در بستر مبادلات الکترونیکی و برروی داده‌ها و اطلاعات وبعضاً (بندرت) بر روی سیستم‌های فیزیکی و سخت افزاری ارتکاب می‌یابد .

در جائیکه جرم سایبر برروی داده‌ها ارتکاب یافته ,تعیین محل ارتکاب جرم کاری بس دشوار ودر برخی موارد حتی غیر ممکن بنظر می‌رسد . محل وقوع جرم سایبری بطور دقیق یعنی محل و مکانی که این داده‌ها دستخوش حملات مجرمانه قرار گرفته ودیگرگون شده‌اند .

چگونه می‌توان یک رخداد غیر فیزیکی ومجازی رادر دنیای فیزیکی و در بعد مکانی جستجو کرد؟

حتی اگر جرم سایبری بر روی قطعات فیزیکی و سخت افزاری ارتکاب یافته و باعث بروز اختلالات و یا از کارافتادگی آنها گردد، باز هم بطور قطع نمی‌توان نظر داد که محل وقوع جرم سایبری همان محل وجود قطعات سخت افزاری آسیب دیده خواهدبود . چرا که در قریب باتفاق اینگونه جرایم , عمل مجرمانه در مکانی دیگر انجام گرفته وتنها نتیجه مجرمانه بر روی قطعات سخت افزاری پدیدار گشته.

در هر صورت ,تعیین محل ارتکاب فعل مجرمانه(سایبری) در فضای مجازی مبادلات داده‌ها، براحتی امکان پذیر نبوده و نیست . برای مثال : کاربری در شهر لندن با مخاطب خود در شهر پاریس ارتباط اینترنتی برقرار نموده و در طی این تماس , با نفوذ غیر مجاز به بانک داده‌های شخص مخاطب خود در پاریس اقدام به سرقت اطلاعات مورد نیاز خود از مخاطب نموده و سپس با تخریب اطلاعات باقیمانده , بانک اطلاعات وی راترک مینماید.

حتی در این مثال ساده نیز نمی‌توان معین نمود محل ارتکاب این جرائم (نفوذ غیرمجاز- سرقت داده ـ تخریب داده) کجاست !

چرا که شخص مرتکب در لندن با استفاده از برنامه‌های خاص نرم افزاری اقدام به نفوذ غیر مجاز به سیستمهای مخاطب خود در شهر پاریس نموده ودر همین حین مرتکب جرائم دیگری نیز برروی داده‌های کاربر فرانسوی گردیده و کاربر فرانسوی بر روی رایانه خود نتیجه این افعال مجرمانه رابصورت بروز اختلالات در برنامه‌ها و سیستمهای خود مشاهده می‌کند. این‌ها همه درحالیست که در واقع پایگاه داده‌ها در شهر تورنتو کانادا واقع است واگر سرقت ,تخریب و هرگونه جرمی بر روی داده‌ها رخ داده باشد در واقع آن پایگاه داده‌ها مورد حمله قرار گرفته و کاربرفرانسوی فقط نمایشی از آنرا در پاریس مشاهده خواهد کرد.

ملاحظه میشود که جرایم محیط سایبر بر خلاف جرایم سنتی که در مکانهای مشخص و یامحصوری اعم از یک اتاق , یک ساختمان و یا یک منطقه رخ میدهند ,ممکن است درچندگوشه کره زمین ارتکاب یابند همچنین با این تفاوت که نه تنها از نقطه نظر فنی وتکنیکی بلکه از نقطه نظر حقوق کیفری نیز نمی‌توان بطور حتم مکان واحدی رابعنوان محل ارتکاب جرم برگزید .

بااین اوصاف تدابیرقوانین دادرسی سنتی که با پارامترهایی همچون محل ارتکاب جرم (صلاحیت سرزمینی) تبیین شده‌اند , کارائی خود را از دست خواهندداد. زیرا اصلاً در وهله نخست شروع به تعقیب و رسیدگی به این جرائم خاص نمیدانیم جرم در کدام حوزه واقع شده تا بنابه اصل صلاحیت سرزمینی اولاً کشورصالح و سپس باتوجه به قواعد پیش بینی شده در قوانین دادرسی , حوزه قضایی صالح راشناسایی نمائیم .

مسئله دوم ـ شناسائی تابعیت شخص مرتکب :

هنگامیکه بحث از تابعیت شخص مرتکب به‌میان می‌آید بلافاصله مفهوم صلاحیت شخصی در آئین دادرسی کیفری به ذهن متبادر می‌شود. اینکه مرتکب دارای چه تابعیتی است در بسیاری موارد کشور متبوع وی را صالح به رسیدگی به اتهامات وی می‌نماید چنانکه در ما ده ۷ قانون مجازات اسلامی نیز رسیدگی به کلیه جرائم ارتکابی توسط ایرانیان در هر کجای جهان را در صلاحیت دادگاههای کیفری داخلی دانسته .

اما در جرائم سایبری ,حتی تابعیت مرتکب نیز ناشناخته است . چرا که در فضای مجازی کاربران باشناسه‌های قرار دادی همچون IP ها (قرار دادهای اینترنتی) که تماماً مجازی وغیر قابل مشاهده و لمس هستند، شناسایی میشوند و حتی در

صورت شناسایی کاربر مرتکب جرم , در واقع ما هویت مجازی و قرار دادی وی راشناسایی کرده‌ایم نه هویت واقعی او را همچنان که در ادارات تشخیص هویت پلیس کشورها صورت می‌پذیرد .

مسئله سوم ـ حل تعارض صلاحیت‌ها:

بدون پاسخ به پرسشهای اول و دوم (که بعداً به آنها اشاره خواهیم کرد) فرضی رادر نظر می‌گیریم که صلاحیت قضایی بیش از یک کشور ویا در سیستم داخلی ,بیش از یک حوزه قضایی در رسیدگی به یک جرم و یا اتهام مرتکب احراز گردیده . ظاهراً این تعارض پدید آمده شبیه به تعارضات سنتی و تابع قواعد حل تعارضات سنتی خواهدبود . اما میدانیم در تعارض صلاحیت‌ها در حالت سنتی ,ابعاد دامنه جرم یاجرائم، مشخص ومحدود است و با توسل به راهکارهای ارائه شده ازجمله استردادو.... تا حد قابل توجهی می‌توان به این تعارضات خاتمه داد. اما نظر به دامنه شمول جرایم موضوع این بحث وفراگیر بودن وامکان ورود خسارات و زیانهای غیر قابل تصور (همانند خواباندن شبکه سراسری برق رسانی یک کشور یا چند کشورهمجوار) دیگر به سادگی قبل نمی‌توان تعارض پیش آمده در صلاحیت دولتهارا حل نمود . چرا که هر دولت آنچنان از این جرایم صدمه دیده که براحتی حاضر نیست از صلاحیت خود صرف نظر نموده و اختیار رسیدگی رابه دولتهای دیگر محول نماید ....

حل مسئله :

در یک رویکرد کلی در خصوص جرایم سایبری می‌بایستی فضای ذهنی قانونگذار را از محیط واقعی و فیزیکی خارج نموده ودر محیط کاملاً مجازی و غیر واقعی قرارداد . از سوی دیگر ماهیت غیر واقعی جرایم سایبری باعث گردیده تا مرزهای جغرافیایی و مفهوم سرزمینهای مجزا، رنگ باخته و اصطلاحاً عبارت «صلاحیت غیر مبتنی برمرز» یا «صلاحیت فرامرزی» جایگزین صلاحیت های مبتنی بر حیطه بندیهای جغرافیایی سیاسی و طبیعی گردد. چرا که ماهیت جرائم سایبر اصولاً ماهیتی فرامرزی بوده و می‌بایست بدون در نظر گرفتن مکان وموقعیت فیزیکی مرتکب، محل ارتکاب و ... مورد بررسی قرار گیرند .

نتیجه : راه حل پیشنهادی درتعیین دادگاه صالح , تنها عبور از قواعد سنتی و در نظر گرفتن موقعیت بزهدیده است . یعنی چنانچه بزهدیده جرائم سایبر به دادگاه کیفری محل اقامت خود، تقدیم شکوائیه نماید دادگاه، تنها بر مبنای اینکه بزهدیده درحوزه آن دادگاه ساکن است می‌باید خود را صالح برسیدگی دانسته و با قبول شکایت، اقدام به تعقیب و رسیدگی قضایی نماید . زیرا تنها محلی که می‌توان تحقیقات مقدماتی را از آنجا آغاز نمود و امکان جمع آوری آثار جرم درآن وجود دارد، محلی است که متهم در آن اقامت داشته وحداقل، نمایشی از وقوع جرم سایبر بر روی داده‌ها ویا سیستمهای او قابل رؤیت می‌باشد.

مشکلی که در پی این قضیه پیش خواهد آمد , تعدد بزهدیدگان ودر نتیجه تعدد مراجع قضایی صالح به رسیدگی خواهدبود . مثلاً در جرم انتشار ویروسهای مخرب رایانه ای که صدها ویا هزاران کاربر را در سطح یک کشور و حتی در سطح جهان، بزهدیدهء خودواقع می‌سازد , چنانچه هریک از بزهدیدگان به دادگاه محل اقامت خود اعلام جرم وتقدیم شکوائیه نماید ,ناگهان دهها دهها مرجع قضایی اقدام به پیگیری , تعقیب و رسیدگی نسبت به یک جرم واحد واحتمالاً بامتهم واحد، خواهند نمود . ناگفته پیداست که مهمترین تبعات چنین اقدامی، تراکم پرونده‌های کیفری در دادگاههای متعدد و تهافت و تعارض آراء صادره خواهد بود .

در سطح جهانی اولاً بنابه پیشنهاد بند ۵ ماده ۲۲ کنوانسیون بوداپست در خصوص کشورهای عضو ,مشورت واتخاذ تصمیم در خصوص صالح دانستن یکی از اعضاء، به رسیدگی به تمامی اتهامات وارده وشکایات واصله خواهد بود و، چه درمورد کشورهای عضو کنوانسیون مزبور، وچه در خصوص کشورهای غیر عضو , بهترین و کارآمدترین راه حل , تقویت همکاریهای بین المللی ویاهمان معاضدت قضایی بین المللی ست که البته کنوانسیون نیز نظر به‌اینکه در قسمت صلاحیت نهایتاً راه حل روشنی ارائه ننموده، بلافاصله پس از مبحث مربوط به صلاحیت ,ذیل فصل سوم ،تحت عنوان همکاریهای بین المللی ,از ماده ۲۳ تا ۳۵ طی ۱۳ ماده اصول همکاریهای قضایی وپلیسی بین المللی راتبیین نموده و حتی درماده ۳۵ ، یک نقطهء تماس بین‌المللی را که بطور ۲۴ ساعته و بصورت On Line آماده دریافت ,پیگیری وارائه گزارشات مربوط به همکاری کشورها درمبارزه با جرائم سایبریست ,برای هریک از اعضاءپیش بینی نموده تا از این طریق باسریع‌ترین وسایل ارتباطی که به آنها نیزتحت بند ۳ ماده ۲۵ قابلیت استناد بخشیده , بتوانند به پیگیری و تعقیب و رسیدگی این جرائم اهتمام ورزند . حتی در رسیدگیهای قضایی با یاد آوری اصول مربوط به استرداد مجرمین (ماده ۲۴) سعی در تقویت معاضدت قضایی دولتها نموده .

و اما در خصوص تعارض صلاحیت در حوزه‌های قضایی داخلی , می‌توان باتأسیس یک هیأت و یاشعبه مرکزی، در خصوص رسیدگی به جرائم سایبر در کشور، که باتوجه به قابلیت‌های تخصصی وامکانات مالی وتجهیزاتی علی القاعده در تهران برپا خواهد شد, به تمامی مراجع قضایی سراسر کشور تکلیف نمود، تا در صورت دریافت هرگونه گزارش از مقامات ذیصلاح و یا وصول شکوائیه و یا مشاهده هرگونه جرمی از جرائم محیط سایبر ,بلافاصله شعبه مرکز ی رادر جریان امر قرار داده و منتظر تعیین تکلیف از سوی شعبه مرکزی بمانند.

با این روش چنانچه بزهدیدگان متعددی در سراسر کشور اقدام به تقدیم شکوائیه نموده و خواستار پیگیری قضیه شده باشند ,تمامی این شکایات واعلامات در شعبه مرکزی منعکس شده و این شعبه، با درنظر گرفتن معیارهای اصولی همچون تراکم بزهدیده در نقطه یا نقاط خاص ,وجود واعلام احتمالی کشف ادله جرم در یک یاچند حوزه خاص، و یا دستیابی احتمالی هر یک از حوزه ها به اطلاعات مرتکب یا مرتکبین , باارجاع پرونده به حوزه‌ایکه بیشترین پارامترها رادر اختیار دارد وهمچنین تکلیف دیگر مراجع گزارش دهنده، به این که تمامی پرونده‌های متشکله و تحقیقات احتمالی انجام گرفته را نزد شعبه مرجوع الیه ارسال نمایند,گامی مؤثر در جهت تعیین مرجع صالح واحد، وجلوگیری از تراکم پرونده در حوزه‌های مختلف واصدار آراء متهافت ومتعارض برداشته خواهدشد .

بدیهیست نظر به سرعت خیره کننده مبادلات در محیط سایبر، و به تبع آن، سرعت ارتکاب جرایم سایبر، وامکان فرار بسیار سریع مرتکب، از صحنه جرم (مجازی)، و امکان اختفاء ویا حتی امهاء آثار ودلایل جرم، این گونه اطلاع رسانی، و ارجاع واحد، بایستی باحداقل تلف زمانی صورت پذیرد که این سرعت عمل امری بایسته و تفکیک ناپذیر، در پیشگیری و مبارزه باجرائم سایبر خواهد بود، انشاء ا... تعالی.

☑ **عنوان: قانون تجارت الکترونیکی و امضای الکترونیکی**

☑ **نویسنده: دکتر ستار زرکلام** (استادیار گروه حقوق دانشگاه شاهد)

مقدمه

یکی از رهاوردهای مهم فناوری اطلاعات[۱]، تحول در رژیم سنتی ادله اثبات دعوا است. در نظام ادله اثبات دعوای اکثریت مطلق کشورهای جهان، پس از اقرار، دلایل کتبی یا نوشته از اهمیت غیر قابل انکاری برخوردار هستند، به‌نحوی که بیشترین استفاده را در مقام استناد یا دفاع از دعوا دارند. در واقع، طرح دعوا و اقامه دلایل در زندگی حقوقی ما تا حدود زیادی منوط به ارائه یا صدور یک نوشته کاغذی نظیر کارت شناسایی، فیش حقوق، رسیدهای پرداخت وجه، قراردادها، اعلامیه‌ها و اخطارها و اظهارنامه‌ها و اسناد تجارتی است. فناوری اطلاعات به دلیل ویژگی‌های فنی خود به‌طور محسوس از گردش کاغذ و دلایل کاغذی می‌کاهد. بدیهی است این فناوری قادر به حذف گردش کاغذ نیست، ولی دامنه آن را روز به روز کاهش خواهد داد. در کشورهای پیشرفته این فرآیند مدتها است که آغاز شده و بانکها و مؤسسات بیمه، بنگاه‌های اداری و تجاری خصوصی یا دولتی با بهره‌گیری از فناوری جدید، سعی در کاستن از حجم گردش کاغذ و تبادل اطلاعات به طریق الکترونیک دارند [۱] تا آنجا که برخی تحقق «دولت الکترونیک» را دور از انتظار نمی‌دانند. با ظهور اینترنت، این پدیده ابعاد بین‌المللی و فرامرزی به خود گرفته است، به نحوی که تجارت الکترونیک اساساً بدون استفاده از دلایل کاغذی انجام می‌شود. در کشور ما نیز استفاده از روش‌های الکترونیک به جای نوشته‌های کاغذی یا اسناد کتبی مدتها است آغاز شده که از آن جمله می‌توان به مکانیزه کردن سیستم اداری مالیاتی، حسابرسی در بخش دولتی و خصوصی، مبادلات الکترونیکی بین بانکی و استفاده از کارتهای بانکی الکترونیک اشاره کرد. توسعه مبادلات الکترونیک و جایگزینی نوشته‌های کاغذی با الکترونیکی بدون شک مسائل حقوقی جدیدی را مطرح می‌کند که مهمترین آنها، اثبات این گونه مبادلات، صحت محتوای ذخیره شده و تعیین هویت طرفین مبادله است. در واقع، زمانی که اشخاص از طریق فناوری اطلاعات مبادرت به اعمال حقوقی می‌کنند، مشکل اساسی در احراز رابطه حقوقی و هویت طرفین از آنجا آغاز می‌شود که: اولاً توافق یا تشکیل قرارداد و تبادل ایجاب و قبول از راه دور و بدون حضور فیزیکی و رو در روی طرفین رابطه حقوقی انجام می‌گیرد. [۲]

ثانیاً آنچه رد و بدل می‌شود داده‌هایی است که کامپیوتر آنها را به زبان قابل فهم تبدیل و به مخاطب ارسال می‌کند. به عبارت دیگر، اعلام اراده در محیطی کاملا مجازی و غیر مادی صورت می‌گیرد. کشورهای پیشرفته و حتی اکثر کشورهای در حال توسعه جهان با سرعت و جدیت تمام در جستجوی راه‌حل‌های حقوقی برای انطباق با مسائل ناشی از فناوری اطلاعات هستند تا خلاءهای قانونی، مانع از تحولی که این فناوری در پی آن است نگردد. بسیاری از این کشورها با تصویب قانون

۱- Information Technology (IT)

تجارت الکترونیکی و یا قانون امضای دیجیتال و مبادلات الکترونیکی [۳، ص ۱۱۹] یا با اصلاح قوانین مدنی خود، قدمهای اساسی در این راه برداشته‌اند که از جمله می‌توان به اصلاح ماده ۱۳۱۶ قانون مدنی فرانسه و مواد ۲۸۳۷ و ۲۸۳۸ قانون مدنی کبک (کانادا) اشاره کرد [۴].

در ایران نیز فراهم ساختن زیرساخت‌های حقوقی امضای الکترونیکی با تصویب قانون تجارت الکترونیک در تاریخ ۸۲/۱۰/۲۹ آغاز شده است. این مقاله درصدد است با بررسی قوانین و مقررات کشورهای مختلف، سازمانهای تجاری بین‌المللی و شورای اروپا نقاط قوت و ضعف مقررات راجع به امضای الکترونیکی را مورد بحث قرار دهد.

مبحث اول – مفهوم و انواع امضای الکترونیکی

اثبات وجود رابطه حقوقی، احراز هویت طرفین این رابطه و تمامیت محتوای اطلاعات رد و بدل شده در محیط الکترونیکی را که غیر مادی و مجازی است ایجاب می‌کند. این امر دست‌اندرکاران حقوق انفورماتیک را به جستجوی «امضای الکترونیکی» یا «امضای انفورماتیکی» هدایت کرده است. برای فهم آنچه امضای الکترونیکی نامیده می‌شود ابتدا تعریف آن ضرورت دارد تا سپس انواع امضای الکترونیکی مورد بررسی قرار گیرد.

۱- مفهوم امضای الکترونیکی

در آنچه به امضای کاغذی مربوط می‌شود هر چند سیستم‌های حقوقی که اساساً هیچ‌گونه توصیف قانونی از امضاء ارائه نمی‌دهند فراوان هستند[۵، ص ۷۸۷]، ولی تعریف سنتی ارائه شده از امضاء در این سیستم‌های حقوقی، وجود یک نوشته را ضروری می‌داند. قانون مدنی ایران در ماده ۱۳۰۱ بدون تعریف امضاء مقرر می‌دارد: «امضایی که روی نوشته یا سندی باشد بر ضرر امضاءکننده دلیل است». از سوی دیگر، برخی از حقوقدانان امضاء را چنین تعریف کرده‌اند: «نوشتن اسم یا اسم خانوادگی (یا هر دو) یا رسم علامت خاصی که نشانه هویت صاحب علامت است. در ذیل اوراق و اسناد عادی یا رسمی که متضمن وقوع معامله یا تعهد یا قرار یا شهادت و مانند آنها است یا بعداً باید روی آن اوراق تعهد یا معامله‌ای ثبت شود (سفید مهر)» [۶، ص ۸۱].

در حقوق فرانسه، آمریکا و انگلیس نیز تعریف مشابهی از امضاء ارائه شده است [۷، ص ۸۱۳]. اما در فضای الکترونیکی که نوشته‌ها تجسم بیرونی و مادی ندارند و تبادل اطلاعات در یک محیط مجازی صورت می‌گیرد، تجدیدنظر در مفهوم امضاء نیز ضرورت خواهد داشت. در این مفهوم، یک رمز، یک پیام یا هر روش غیر مادی می‌تواند تحت شرایطی از ارزش اثباتی امضا به مفهوم سنتی آن برخوردار شود [۲، ص ۱۱۱۳]. امضای الکترونیکی به مفهوم عام کلمه عبارت است از یک رمز مستقل و محرمانه که تعیین هویت ارسال کننده و الحاق او به سندی که محتوای داده را تشکیل می‌دهد ممکن است [۲، ص ۱۱۱۳]. از امضای الکترونیکی تعاریف مختلف و متفاوتی ارائه شده است. به عنوان مثال، قانون نمونه کمیسیون سازمان ملل برای حقوق تجارت بین‌المللی (آنسیترال) مقرر می‌دارد: «هرگاه قانون وجود امضاء را ضروری بداند، داده پیام امضاء شده محسوب می‌شود، اگر: الف) از روشی برای تعیین هویت شخص و تأیید اطلاعات موجود در داده پیام استفاده شود و ب) از روش به کار گرفته شده متناسب با موضوعی که داده پیام برای آن ایجاد یا ارسال شده، با توجه به اوضاع و احوال از جمله هرگونه توافق خصوصی اطمینان حاصل شود» [۱۰، ص ۱۶۷۴]. در مقابل، براساس دستورالعمل شماره ۱۹۹۹/۹۳/CE پارلمان و شورای اروپا مورخ ۱۳

دسامبر ۱۹۹۹، منظور از امضای الکترونیکی، داده‌ای الکترونیکی است که به سایر داده‌های الکترونیکی متصل یا منطقاً مرتبط بوده، روشی برای احراز اصالت به شمار می‌رود. [۸، ص ۱۷۹۴].

قانون مدنی فرانسه در قسمت دوم ماده ۴- ۱۳۱۶ پس از تعریف امضا، در انطباق با دستورالعمل اروپایی مصوب ۱۳ دسامبر ۱۹۹۹، امضای الکترونیکی را چنین تعریف می‌کند: «در صورتی که امضاء الکترونیکی باشد، این امضا در عمل عبارت از رویه مطمئنی است که شناسایی رابطه امضاء را با سندی که منضم به آن است تضمین می‌کند. اصل بر مطمئن بودن این رویه است، مگر آنکه دلیل مخالفی در بین باشد. هنگامی که امضای الکترونیکی انجام می‌شود، هویت امضاءکننده و تمامیت سند را با توجه به شرایط مقرر در مصوبه شورای دولتی تضمین می‌کند» [۴، ص ۹۷]. برابر بند «ی» از ماده ۲ قانون تجارت الکترونیکی ایران «امضای الکترونیکی عبارت از هر نوع علامت منضم شده یا به نحو منطقی متصل شده به داده پیام است که برای شناسایی امضاکننده داده پیام مورد استفاده قرار می‌گیرد» [۹، ص ۴].

دقت در این تعاریف نشان می‌دهد برخی از آنها نظیر مقررات آنسیترال و حقوق فرانسه بیشتر بر جنبه‌های حقوقی امضاء تأکید دارند، در حالی که برخی دیگر، نظیر تعریف پارلمان و شورای اروپا، ناظر بر جنبه‌های مادی امضاء هستند. تعریف قانون تجارت الکترونیکی ایران از امضای الکترونیکی با قانون نمونه آنسیترال نزدیکی بیشتری دارد. با این حال همه این تعاریف در وجوه زیر مشترک هستند:

اول، امضای الکترونیکی، یک داده الکترونیکی است؛ دوم، این داده به داده‌های الکترونیکی نیز منضم می‌شود یا منطقاً با آن مرتبط است؛ سوم، این امضاء رابطه امضاکننده را با داده‌هایی که با آن مرتبط است مشخص می‌کند.

۲- انواع امضای الکترونیکی

قانون تجارت الکترونیکی دو سطح مختلف از امضای الکترونیکی را پذیرفته است. اول امضای الکترونیکی که می‌توان آن را «ساده» یا «عادی» نامید و تعریف آن فوقاً ارائه شد و دوم «امضای الکترونیکی مطمئن» که مطابق ماده ۱۰ قانون باید دارای چهار شرط باشد: نسبت به امضاء کننده منحصر به فرد باشد، هویت امضاء کننده داده پیام را معلوم کند، به وسیله امضاکننده و یا تحت اراده انحصاری او صادر شده باشد و به نحوی تولید و متصل به داده شود که هر تغییری در داده پیام قابل تشخیص و کشف باشد [۹]. امضای الکترونیکی مطمئن به لحاظ فنی یا یک امضای دیجیتال است[۱۰، ص ۵۱ و بعد] و یا یک فرآیند تجاری معقول که طرفین آن را به رسمیت شناخته‌اند.[۳، ص ۱۳]. امضای دیجیتال یک فرآیند رمزنگاری[۲] است که از یک جفت کلید موسوم به کلید اختصاصی[۳] و کلید عمومی[۴] تشکیل می‌شود. کلید اختصاصی به دارنده آن اختصاص دارد و کلید عمومی در اختیار دریافت کننده (مخاطب) فرضی قرار می‌گیرد. این دو کلید از نظر ریاضی کاملاً با هم مرتبط و به هم پیوسته هستند و در جهان خارج کاملاً تک. یکی از آن دو (کلید اختصاصی) برای امضای دیجیتال و دیگری (کلید عمومی)

۲- Cryptography

۳- Private key

۴- Public key

برای تطبیق و سنجش کلید اختصاصی به کار می‌رود. امضای دیجیتال یک فناوری رمزنگاری نامتقارن[۵] است؛ یعنی در آن از دو کلید متفاوت برای رمز و کشف رمز پیام استفاده می‌شود [۱۰، ص ۵۱ و بعد].

قانون مدنی فرانسه تفاوتی بین امضای الکترونیکی ساده و مطمئن قائل نشده است، ولی شورای دولتی فرانسه که نحوه تعیین هویت امضاءکننده و نیز تضمین تمامیت سند به آن واگذار شده (ماده ۴- ۱۳۱۶) در مصوبه خود بین امضای الکترونیکی و امضای الکترونیکی مطمئن قائل به تفکیک شده است. برابر ماده ۱ این مصوبه، امضای الکترونیکی (ساده) عبارت از به کارگیری رویه قابل اعتماد در تعیین هویت است که رابطه‌اش را با سندی که به آن منضم است تضمین می‌کند. در مقابل امضای الکترونیکی مطمئن، امضایی است که علاوه بر دارا بودن شرایط امضای الکترونیکی مطمئن، امضایی است که علاوه بر دارا بودن شرایط امضای الکترونیکی (ساده)، اولاً توسط روش‌هایی ایجاد شود که در کنترل انحصاری امضاکننده باشد و ثانیاً رابطه امضاء را با سندی که منضم به آن است تضمین کند، به نحوی که هرگونه تغییر بعدی در سند قابل کشف باشد. براساس ماده ۲ همین مصوبه، روش‌های فنی تولید امضای الکترونیکی مطمئن باید تک بودن، محرمانه بودن، تمامیت سند و قابل شبیه‌سازی نبودن را تضمین کند [۸، ص ۱۷۹۷].

به موجب ماده ۲۸۳۷ قانون مدنی کبک: «زمانی که داده‌های یک سند حقوقی بر روی قالب انفورماتیکی ثبت شده‌اند، مدرک حاکی از این داده‌ها، دلیل محتوای سند است؛ مشروط بر اینکه این مدرک، هوشمند باشد و تضمین‌های جدی برای این که بتوان به آن اعتماد کرد موجود باشند».

ماده ۲۸۳۸ همین قانون مقرر می‌دارد «با ثبت داده‌ها بر روی قالب انفورماتیکی، وجود تضمین‌ها جدی برای اعتماد به آنها مفروض است، به شرط اینکه به‌طور سیستماتیک و بدون خلاء باشد و داده‌های ثبت شده در مقابل هرگونه خدشه‌ای حمایت شده باشند». در واقع قانون مدنی کبک به نحو دیگری صحبت از امضای الکترونیکی مطمئن می‌کند [۴، ص ۹۷]

نگاهی به قوانین و مقررات فوق نشان می‌دهد که قانونگذاران کشورهای مختلف از طریق امضای الکترونیکی بخصوص با وصف «مطمئن» درصدد هستند که ویژگی‌های یک سند کاغذی، یعنی تمامیت، دوام و امکان انجام امضاء بر روی قالب را تضمین کنند. در محیط الکترونیک یا دیجیتال، تمامیت یک سند. دوام و رابطه‌اش با فایل‌های حاوی امضاء تماماً بستگی به کارایی سیستم مورد استفاده دارد [۲، ص ۱۳].

مبحث دوم- مستندسازی امضای الکترونیکی(دفاتر خدمات صدور گواهی الکترونیکی)

با استفاده از روش امضای دیجیتال یا امضای مبتنی بر رمزنگاری نامتقارن [۱۰، ص ۵۱ و بعد] تمامیت سند، محرمانه بودن اطلاعات (در صورت لزوم) و امنیت داده‌ها تضمین می‌شود؛ اما یک مسأله مهم حل نشده باقی می‌ماند و آن، تضمین هویت امضاء کننده است. در واقع به لحاظ حقوقی، مهمترین اثر امضاء اثبات رابطه سند با کسی است که امضاء به او نسبت داده شده است. امضای الکترونیکی مطمئن یا دیجیتال به تنهایی قادر به تضمین هویت امضاءکننده نیست. آنجا که طرفین رابطه حقوقی تجار بزرگ بین‌المللی یا شرکت‌های چند ملیتی هستند، این مشکل کمتر بروز می‌کند؛ زیرا طرفین یکدیگر را به

۵- Asymetric Cryptography

خوبی می شناسد و از توانایی‌های مالی و فنی و انسانی یکدیگر به خوبی آگاه هستند. در این گونه موارد، صرف مبادله داده‌های رمزنگاری شده برای اثبات وجود رابطه حقوقی و محتوای آن کفایت می‌کند. همچنین در مواردی که طرفین مبادله الکترونیکی قبل از ورود به محیط الکترونیکی در خصوص نحوه انجام این مبادلات و حقوق و تکالیف خود توافق می‌کنند و هویت هر یک از طرفین برای طرف دیگر آشکار است، مشکل تعیین هویت اساساً فرصت بروز نمی‌یابد. به عنوان مثال در عملیات بانکی از طریق کارتهای بانکی الکترونیکی معمولاً مشتری با حضور در بانک، ضمن ارائه مدارک لازم برای تعیین هویت، قراردادی را که بانک در خصوص نحوه استفاده از کارت بانکی و مسائل حقوقی مرتبط با آن، از جمله دلیل انجام عملیات بانکی تهیه کرده، امضاء می‌کند. در این گونه موارد، امضای الکترونیکی می‌تواند مبنایی برای سیستم پرداخت الکترونیکی باشد. در این سیستم دارنده کارت، فروشنده و بانکهای عضو که مبادله را پردازش می‌کنند یک امضای دیجیتال در دست دارند که هویت و صلاحیت وی را درون سیستم تضمین می‌کند.

اما مشکل تعیین هویت در سیستم‌های باز که طرفین از پیش در خصوص حقوق و تکالیف خود توافق نکرده‌اند و همدیگر را نمی‌شناسند همچنان باقی است. به عنوان مثال، در معاملات از طریق شاهراه‌های اطلاعاتی (اینترنت) که در یک طرف آن تجار، شرکتها و مؤسسات تجاری و خدماتی و در طرف دیگر عمدتاً مصرف‌کنندگان قرار دارند، تضمین هویت امضاءکنندگان ضرورت دارد. ا زاین رو از زمانی که فناوری امضای الکترونیکی مطرح شده، یکی از دغدغه‌های اصلی قانونگذاران ملی و سازمان‌های تجاری بین‌المللی و اتاق‌های بازرگانی این است که مرجع ثالثی، اعتبار پیام را از طریق تعیین هویت امضاءکننده دیجیتال تضمین کند. این مرجع ثالث اصطلاحاً «دفاتر خدمات صدور گواهی الکترونیکی» یا «دفاتر خدمات الکترونیکی» یا «مراجع گواهی» نامیده می‌شود. عملکرد این دفاتر با عملکرد دفاتر اسناد رسمی در محیط نوشته‌ها و اسناد کاغذی قابل مقایسه است. به عبارت دیگر، همان‌طور که دفاتر اسناد رسمی با احراز هویت امضاکنندگان سند و طی تشریفات قانونی به نوشته سندیت و رسمیت می‌بخشند، «دفاتر گواهی الکترونیکی» نیز هویت امضاءکننده را تضمین می‌کنند و نتیجتاً به اطلاعات الکترونیکی سندیت می‌دهند. در واقع، گواهی دیجیتال که توسط دفاتر خدمات الکترونیکی صادر می‌شود، هویت امضاکننده را از طریق کنترل رابطه بین کلید عمومی و دارنده کلید خصوصی مربوط تضمین می‌کند. به عبارت دقیق‌تر، امضای دیجیتال دارای دو جز متفاوت، اما از نظر ریاضی مرتبط است. کلید خصوصی که در اختیار صاحب امضا است و کلیدی عمومی که در فهرست مرجع گواهی قرار دارد. این مرجع تضمین می‌کند که کلید عمومی مستقر در فهرست به درستی اعلام و ایجاد شده است؛ زیرا هویت دارنده کلید خصوصی که منطبق با کلید عمومی است نزد مرجع گواهی وجود دارد. برای اطمینان از اینکه داده پیام از سوی کسی که ادعا می‌کند صادر شده، وجود کلید عمومی ضروری است. در واقع، مرجع گواهی دو وظیفه مهم دارد: اول، تخصیص یک کلید خصوصی به دارنده و ثبت آن به عنوان یک مستند اطلاعاتی؛ و دوم نگهداری کلید مکمل آن به نام کلید عمومی و در دسترس قرار دادن فهرست نام دارندگان کلید عمومی از طریق سیستم درون خطی و بانکهای اطلاعاتی ویژه [۱۱، ص ۱۱۸ و بعد].

این گواهی برای اینکه معتبر شناخته شود به علاوه باید متضمن موارد دیگری از قبیل هویت خود مرجع گواهی، مدت اعتبار گواهی، شماره سری گواهی و موارد دیگر باشد [۱۲، ص ۱۶۰۰۲ و بعد] که ذکر همه موارد و توضیح آنها در حوصله این مقاله نمی‌گنجد.

تأسیس دفاتر خدمات صدور گواهی برای تأیید و تصدیق داده‌های منضم به امضاء و ارائه گواهی لازم در دستورالعمل شماره ۱۹۹۹/۹۳/CE مورخ ۱۳ دسامبر ۱۹۹۹ پارلمان و شورای اروپا پیش‌بینی شده است. ماده ۲ این دستورالعمل، دولتهای عضو را مجاز می‌سازد نسبت به تأسیس دفاتر خدمات الکترونیکی و یا نگاهداری دفاتر موجود، طبق شرایط مندرج در دستورالعمل اقدام کنند[۸، ص۱۷۹۴]. بر این اساس، مصوبه شماره ۲۷۲-۲۰۰۱ مورخ ۳۰ مارس ۲۰۰۱ شورای دولتی فرانسه ضمن تعریف گواهی الکترونیکی (بند ۹ ماده ۱) و گواهی الکترونیکی معتبر (بند ۱۰ ماده ۱)، شرایط لازم برای گواهی الکترونیکی معتبر را برشمرده است (ماده ۶) [۸، ص ۱۷۹۷].

قانون تجارت الکترونیکی بدون اینکه تعریفی ازگواهی الکترونیکی ـ در فصل دوم خود راجع‌به تعاریف ـ ارائه دهد، باب دوم خود را به تأسیس «دفاتر خدمات صدور گواهی الکترونیکی» اختصاص داده و با تعریف این دفاتر، ضوابط تأسیس و شرح وظایف آنها را به آیین‌نامه موکول کرده است [۹].

براساس پیش‌نویس اولیه قانون تجارت الکترونیکی، گواهی الکترونیکی باید توسط دفاتر یا مراکزی صادر شود که از صلاحیتهای لازم برای ارائه این گونه خدمات برخوردار باشند. شرایط لازم برای صدور مجوز فعالیت این دفاتر و نیز مراکز یا سازمان‌هایی که می‌توانند این مجوزها را صادر و بر نحوهٔ فعالیت دفاتر گواهی نظارت کنند، مطابق قوانین هر کشور تعیین می‌شوند، به عنوان مثال ماده ۴۱ این پیش‌نویس، دفاتر خدمات صدور گواهی الکترونیکی را واحدی وابسته به وزارت بازرگانی می‌دانست که به مدیریت و مسئولیت یک نفر صاحب دفتر که دفتردار نامیده می‌شود اداره می‌گردد. براساس همین پیش‌نویس، صدور جواز، گواهی، دیده‌بانی و سرپرستی فعالیت‌های دفاتر خدمات گواهی الکترونیکی به عهده دفتردار کل است که توسط وزیر بازرگانی منصوب می‌شود[۳، صص ۱۴۳-۱۴۴]. اما باید دید آثار حقوقی امضای الکترونیکی اعم از ساده یا مطمئن کدامند؟ به عبارت دیگر، دلایل الکترونیکی در مقایسه با ادله سنتی اثبات دعوا از چه ارزش و اعتبار حقوقی برخوردار هستند؟

مبحث سوم – ارزش اثباتی امضای الکترونیکی

همان طور که گفته شد، امضای الکترونیکی برخلاف امضای دستی یا مندرج در اسناد کاغذی، در یک محیط الکترونیکی و با استفاده از روشها و فناوریهای الکترونیکی ایجاد می‌شود. برای اینکه چنین امضایی در مقام دعوا یا دفاع قابل استفاده باشد ضروری است که برخی از ویژگی‌های مهم امضای دستی، یعنی تک (منحصر به فرد) بودن، تعیین هویت، تحت کنترل داشتن و امکان ممیزی را حائز باشد. بدین منظور هر روزه بر کیفیت استانداردهای فنی که چنین خصوصیاتی را تضمین کنند افزوده می‌شود. با این حال، تفاوتهای زیادی بین نوشته‌های الکترونیکی و اسناد کاغذی وجود دارند که باعث تفاوت در آثار حقوقی هر یک از دو نوشته می‌شود. از جمله این تفاوتها این است که اسناد کاغذی در اصل نمونه‌های فیزیکی بی‌مانند هستند، حال آنکه داده الکترونیکی نامحسوس بوده، به سادگی قابل تغییر است. از سوی دیگر، در اسناد کاغذی، وضعیت ذخیره شده و وضعیت قابل قرائت یکسان است. سند کاغذی بی‌واسطه قابل قرائت است و ذخیره‌سازی اغلب به زبانی انجام می‌شود که کاربر بدون آموزش ویژه آن را درک می‌کند و سرانجام اینکه دستکاری یک سند کاغذی باید فیزیکی باشد و روی کاغذ قابل تشخیص است، در حالی که دستکاری الکترونیکی را به کمک چشم نمی‌توان کشف کرد[۱۳، ص ۴۲].

برای بررسی موضوع، ضرورت دارد مواردی را که طرفین مبادله الکترونیکی در خصوص نحوه این مبادله و ارزش اثباتی آن توافق کرده‌اند و اصطلاحاً به آن سیستم بسته می‌گویند از مواردی که چنین توافقی بین طرفین مبادله الکترونیکی وجود

ندارد و از آن به سیستم باز تعبیر می‌شود تفکیک کنیم[۳، ص ۱۸ و بعد]. منظور از سیستم بسته این است که طرفین از پیش در خصوص ارزش اثباتی امضای الکترونیکی و عنداللزوم بار اثبات دلیل توافق کرده باشند. ارزش اثباتی دلایل در چارچوب این سیستم باید جداگانه و به‌طور مفصل مورد بحث قرار گیرد.

در مقابل، سیستم باز، سیستمی است که در آن هیچ‌گونه توافق قبلی راجع‌به امضای الکترونیکی، نحوه ایجاد ومیزان دلالت آن وجود ندارد. در چارچوب این سیستم اصولاً طرفین همدیگر را نمی‌شناسند و از موقعیت اقتصادی یکدیگر با خبر نیستند. رابطه حقوقی بین ارائه کنندگان کالا و خدمات و مصرف‌کنندگان اغلب در چنین محیطی شرکت می‌گیرد. بدیهی است طرفین رابطه حقوقی که از طریق اینترنت یا شاهراه‌های اطلاعاتی با هم مرتبط می‌شوند برای هرگونه مبادله کالا و خدمات با پول باید از هویت یکدیگر آگاهی یابند، از درستی و دقت اطلاعاتی که رد و بدل می‌شود و نیز تمامیت این اطلاعات اطمینان حاصل کنند. سرانجام و مهمتر از همه ضروری است که هرگونه تعهد یک جانبه یا چند جانبه و نیز هرگونه ایجاب و قبولی قابلیت استناد داشته باشد تا در مقام دعوی یا دفاع بتوان از آن استفاده کرد. در غیاب هرگونه توافق قبلی بین طرفین ـ براساس اسناد کاغذی ـ وجود مقررات و قوانینی که توقعات مبادلات الکترونیکی را به نحوی که گفته شد پوشش دهد و پاسخگوی انتظارات طرفین مبادله باشد ضرورت دارد. از این رو تقریباً از سال ۱۹۹۷ به بعد اکثر کشورهای پیشرفته و صنعتی دنیا حتی برخی از کشورهای در حال توسعه، قوانینی را تحت عناوین مختلف نظیر «قانون امضای دیجیتال»، «قانون امضای الکترونیکی»، «قانون ارتباطات الکترونیکی» و امثال آن به تصویب رسانده‌اند. سازمانهای بین‌المللی نظیر سازمان ملل و اتحادیه اروپا و هم‌چنین برخی از مراکز غیر دولتی، مانند کانون وکلای آمریکا هم مقرراتی را در این خصوص تنظیم کرده آند [۳، ص ۱۴۱].

در اکثر قریب به اتفاق این مقررات، آنچه مشترک است تعیین ارزش اثباتی امضای الکترونیکی و یا به عبارت دیگر، اعتبار حقوقی این امضاء و جایگاه آن در میان ادله اثبات دعوای سنتی کشورها است.

ماده ۹ قانون نمونه آنسیترال (کمیسیون سازمان ملل برای حقوق تجارت بین‌المللی) مصوب ۱۹۹۶ از یک سو مقرر می‌دارد که امضای الکترونیکی به این دلیل که به صورت داده پیام است و یا به دلیل اینکه داده پیام فاقد اصل است نباید مردود اعلام شود و از سوی دیگر، برای امضای الکترونیکی قائل به قدرت اثباتی است که براساس قابلیت اطمینان، روش ایجاد امضاء، نگهداری و ارسال پیام، حفظ تمامیت اطلاعات، هویت ارسال کننده و سایر ملاحظات ارزیابی می‌شود [۸، ص ۱۶۷۴]. دستورالعمل مورخ ۱۳ دسامبر ۱۹۹۹ اتحادیه اروپا نیز در ماده ۵ خود تحت عنوان «آثار حقوقی امضای الکترونیکی» دولتهای عضو را موظف می‌سازد که اولاً برای امضای الکترونیکی پیشرفته (مطمئن) همان آثاری را بشناسند که برای امضای دستی قائل هستند و ثانیاً آن را به عنوان دلیل در دادگاه مورد پذیرش قراردهند. بند ۲ این ماده برای امضای ساده نیز ارزش اثباتی قائل شده ودولتهای عضو را از اینکه چنین امضایی را به دلیل قالب الکترونیکی آن یا فقدان گواهی تأیید شده مردود اعلام کنند منع می‌کند [۸، ص ۱۷۹۴].

قانون مورخ ۱۳ مارس ۲۰۰۰ فرانسه راجع‌به انطباق حقوق دلایل با فناوری اطلاعاتی و راجع‌به امضای الکترونیکی که به تبعیت از دستورالعمل اروپایی مورخ ۱۳ دسامبر ۱۹۹۹ تدوین شده به شکل روشنتر ارزش اثباتی امضای الکترونیکی را تبیین کرده است.

براساس ماده ۱ـ۱۳۱۶ قاون مدنی (اصلاحی) فرانسه، «نوشته الکترونیکی» نیز همانند نوشته کاغذی به عنوان دلیل پذیرفته می‌شود، به این شرط که هویت شخص صادر کننده آن را مشخص سازد و تمامیت آن را تضمین کند. ماده ۳ ـ ۱۳۱۶ در تکمیل ماده ۱ـ۱۳۱۶ همان قانون مقرر می‌دارد: «نوشته الکترونیکی از قدرت اثباتی نوشته کاغذی برخوردار است». فایده اصلی این تشبیه، وارد کردن دلیل انفورماتیکی در سیستم اثباتی سنتی است، بدون اینکه جایگاه خاصی برای آن در نظر گرفته شود. بدین ترتیب، امضای الکترونیکی انجام ساده‌ترین اعمال و در عین حال وارد شدن در پیشرفته‌ترین بخشهای تجارت الکترونیکی را ممکن می‌سازد. با این حال، تشبیه دلایل الکترونیکی با دلایل کاغذی دو نتیجه دربردارد: اول اینکه امضای الکترونیکی باید از تضمینهای نوشته‌های کاغذی برخوردار باشد و دوم اینکه قواعد فعلی مرتبط با دلایل کاغذی در کوچک‌ترین اجزای خود در خصوص امضای الکترونیکی اعمال شود [۲، ص ۱۱۱۷].

پیش نویس اولیه قانون تجارت الکترونیکی ایران در فصل هشتم و نهم خود از مقررات قانون مدنی فرانسه هم فراتر رفته بود. ماده ۱۵ این پیش‌نویس صراحتاً مقرر می‌داشت: «کلیه داده‌هایی که به طریقی مطمئن ایجاد و یا نگهداری شده‌اند از حیث محتویات و امضای مندرج در آن، تعهدات طرفین با طرفی که تعهد کرفده و کلیه اشخاص که قائم مقام قانونی آنان محسوب می‌شوند، اجرای مفاد آن و سایر آثار در حکم اسناد رسمی است». مطابق ماده ۱۹ پیش‌نویس هم که ظاهراً به عنوان تأکید ذکر شده بود، ارزش اثباتی داده‌هایی که به طریق مطمئن ایجاد شده‌اند معادل اسناد رسمی تلقی شده بود [۳، ص ۱۴۱]. در حال حاضر هر چند قانون تجارت الکترونیکی در ماده ۱۴ خود داده پیام مطمئن را نه در «حکم اسناد رسمی» بلکه در «حکم اسناد معتبر و قابل استناد» می‌داند، ولی در ماده ۱۵ صراحتاً مقرر می‌دارد که: «نسبت به داده پیام مطمئن، سوابق الکترونیکی مطمئن و امضای الکترونیکی مطمئن، انکار و تردید مسموع نیست و تنها می‌توان ادعای جعلیت به داده پیام مزبور نمود یا ثابت نمود که داده پیام مزبور نمود یا ثابت نمود که داده پیام مزبور به جهتی از جهات قانونی از اعتبار افتاده است». به عبارت دیگر، مقنن رأی داده پیام مطمئن اثری را می‌شناسد که فقط مخصوص اسناد رسمی است.

همان‌طور که ملاحظه می‌شود در مقایسه با دستورالعمل اتحادیه اروپا و حقوق فرانسه که قدرت اثباتی نوشته الکترونیکی را در حد نوشته کاغذی دانسته‌اند، قانون تجارت الکترونیکی در واقع برای نوشته‌های الکترونیکی مطمئن، ارزش اثبتی معادل اسناد رسمی قائل شده؛ هر چند که از عبارت مبهم و غیر حقوقی «اسناد معتبر و قابل استناد» استفاده کرده است.

ممکن است در وهله اول چنین تدبیری اغراق‌آمیز به نظر برسد، ولی دقت در ویژگی‌های امضای الکترونیکی مطمئن که در ماده ۱۰ قانون به آنها اشاره شده و قبلاً در خصوص آن بحث کردیم، شناسایی چنین اثری را برای دلیل الکترونیکی مطمئن کاملاً توجیه می‌کند. در واقع، نحوه ایجاد امضای الکترونیکی مطمئن که اصولاً و در حال حاضر یک امضای دیجیتال و بر رمزنگاری نامتقارن کلید عمومی و خصوصی استوار است [۱۰، ص ۵۱ و بعد] و تأیید آن توسط دفاتر خدمات صدور گواهی الکترونیکی که نقش دفترخانه‌های اسناد رسمی در محیط الکترونیکی را ایفا می‌کنند، چنان اعتباری به امضای الکترونیکی و داده‌های منضم به آن اعطا می‌کند که نه تنها کلیه آثار مادی امضای دستی از قبیل دوام، اصا لت و تعیین هویت امضاء کننده آن را در آن می‌توان یافت، بلکه با توجه به زیرساخت‌های فنی، چنین امضایی کمتر از امضای کاغذی در معرض تغییر و شبیه‌سازی قرار دارد. حتی اگر با توجه به جوان بودن فناوری امضای دیجیتال این نگرانی برای محاکم وجود داشته باشد که ممکن است چنین امضایی مورد سوء استفاده قرار گیرد و مسائل مرتبط با نظم عمومی و حاکمیت دولت را تحت تأثیر قرار دهد، این نگرانی با توجه به ماده ۶ قانون تجارت الکترونیکی رفع خواهد شد، زیرا براساس بندهای «الف» تا «ج» این ماده،

مستثنیات قلمرو داده‌های الکترونیکی شمرده شده است. به موجب ماده ۶ قانون «هرگاه وجود یک نوشته از نظر قانون لازم باشد «داده پیام» در حکم نوشته است، مگر در موارد زیر:

الف) اسناد مالکیت اموال غیر منقول،

ب) فروش مواد دارویی به مصرف‌کنندگان نهایی،

ج) اعلام، اخطار، هشدار و یا عبارات مشابهی که دستور خاصی برای استفاده کالا صادر می‌کند و یا از به کارگیری روش‌های خاصی به صورت فعل یا ترک فعل منع می‌کند» [۹].

با توجه به چنین خصوصیاتی، مواد ۱۴ و ۱۵ قانون تجارت الکترونیکی از این حیث که داده‌های امضای الکترونیکی مطمئن و داده‌های منضم با آن را از حیث برخی آثار در حکم سند رسمی دانسته با منطق حقوقی سازگار است. به علاوه اگر دلایل الکترونیکی مطمئن رادر حکم سند رسمی بدانیم، این تدبیر مانع از آن خواهد شد که چنین دلیلی به راحتی مورد انکار یا تردید قرار گیرد و در نتیجه استنادکننده به دلیل الکترونیکی، هر بار مجبور شود صحت و اعتبار آن را اثبات کند؛ امری که نه تنها موجب کاهش دامنه مبادلات الکترونیکی و تجارت الکترونیکی، بلکه موجب اطاله دادرسی و صرف وقت و هزینه خواهد شد.

نکته مهم دیگری که باید مورد مطالعه قرار گیرد این است که درصورت تعارض بین دلیل الکترونیکی و دلایل سنتی، این تعارض چگونه قابل حل است؟

مبحث چهارم – تعارض امضای الکترونیکی سایر دلایل

همان‌طور که در چارچوب نظام سنتی ادله اثبات دعوا ممکن است دلایل ابرازی توسط طرفین دعوا در تعارض با هم قرار گیرند این امکان نیز وجود دارد که در مقابل استناد یکی از طرفین به اطلاعات الکترونیکی منضم به داده‌های امضای الکترونیکی، طرف مقابل به یکی از ادله سنتی اشاره شده در قوانین موجود استناد کند تا حسب مورد، ارزش محتوای نوشته الکترونیکی را مخدوش کند یا از تأثیر آن بکاهد.

تعارض بین ادله سنتی از یک سو با توجه به ارزشی که قانون برای هر دلیل نسبت به دلایل دیگر مشخص کرده و از سوی دیگر با توجه به دلالت هر یک از این ادله از نظر قاضی برای اثبات دعوا یا دفاع از آن درمقایسه با دلیل معارض مرتفع می‌شود. به‌طور مثال به موجب ماده ۱۳۰۹ قانون مدنی ایران در مقابل سند رسمی یا سندی که اعتبار آن در محکمه محرز شده، دعوایی که مخالف با مفاد و مندرجات آن باشد به شهادت شهود اثبات نمی گردد. هر چند ماده ۱۳۰۹ براساس نظریه مورخ۶۷/۸/۸ شورای نگهبان مخالف شرع شناخته شده است، ولی برخی از حقوقدانان با این استدلال که چون صلاحیت شورای نگهبان در ابطال مستقیم قانون، آن هم خارج از آیین پیش‌بینی شده در قانون به شدت مورد تردید و انکار است، این ماده را همچنان معتبر می‌دانند [۴، ص ۳۰۷].

همچنین ماده منسوخ ۱۳۰۸ قانون مدنی سابقاً مقرر می‌داشت که دعوی سقوط از قبیل پرداخت دین، اقاله، فسخ، ابراء و امثال آن در مقابل سند رسمی یا سندی که اعتبار آن در محکمه محرز شده، ولو آنکه موضوع سند کمتر از پانصد ریال باشد به شهادت قابل اثبات نیست. بالاخره نظر به ماده ۱۳۲۴ قانون مذکور، امارات قضایی تنها در دعاوی‌ای که به شهادت قابل اثبات

است یا زمانی که ادله دیگر را تکمیل می‌کند قابل استناد است. به عبارت دیگر، در مقابل سند رسمی یا اسناد عادی در حکم سند رسمی، اماره قضایی قابل استناد نیست.

حال باید تعارض بین دلایل الکترونیکی و دلایل سنتی چگونه قابل رفع خواهد بود؟ قانون نمونه آنسیترال مصوب ۱۹۹۶ دربند ۲ از ماده ۹ خود بدون تفکیک بین امضای الکترونیکی مطمئن و ساده پیش‌بینی می‌کندکه قدرت اثباتی داده‌های الکترونیکی با توجه به میزان اطمینان به روش ایجاد، نگهداری یا مبادله داده‌ها و همچنین با توجه به روش محافظت از تمامیت اطلاعات و نحوه شناسایی فرستنده پیام و سایر ملاحظات مرتبط سنجیده می‌شود [۸، ص ۱۶۷۴]. مقررات آنسیترال در واقع با مقرره فوق، تعیین ارزش دلایل الکترونیکی در مقایسه با سایر دلایل را به قاضی سپرده تا با در نظر گرفتن معیارهای فوق در این خصوص تصمیم‌گیری کند.

در حقوق فرانسه ماده ۲ـ ۱۳۱۶ قانون مدنی مقرر می‌دارد: «اگر قانون حاوی اصول دیگری نباشد و درصورت فقدان قرارداد بین طرفین، قاضی با توسل به وسایل گوناگون و صرف‌نظر از قالب دلایل، تعارض دلایل ادبی یا کتبی را با تعیین دلیلی که مقرون به صحت است مشخص خواهد کرد»[۱۵، ص ۱۱۰۵].

با توجه به ماده فوق‌الذکر قاضی تنها زمانی تعارض دلایل را حل و فصل خواهد کرد که در این خصوص توافقی بین طرفین وجود نداشته باشد. به عبارت دیگر، چنانچه طرفین در خصوص ارزش اثباتی دلایل الکترونیکی در مقایسه با دلایل دیگر توافق کرده باشند قاضی الزاماً باید مطابق این توافق عمل کند. به نظر برخی از حقوقدانان فرانسوی، این ماده اولاً هرگونه تفوق نوشته کاغذی بر نوشته الکترونیکی را منتفی می‌داند و ثانیاً صراحتاً بر اعتبار قراردادهای خصوصی در زمینه دلایل صحه می‌گذارد [۱۶، صص ۵۸۲-۵۸۳].

قانون تجارت الکترونیکی ایران با توجه به محدودیت‌هایی که در حقوق ایران برای توافق در خصوص دلایل وجود دارد طبیعتاً نم ی‌توانسته از الگوی فرانسوی پیروی کند. از این رو در حقوق ایران همانند قانون نمونه آنسیترال در خصوص دلایل الکترونیکی ساده باید ماده ۱۳این قانون تجارت الکترونیکی را حاکم دانست که به موجب آن: به‌طورکلی، ارزش اثباتی «داده پیام» با توجه به عوامل مطمئنه از جمله تناسب روش‌های ایمنی به کار گرفته شده با موضوع و منظور مبادله «داده پیام» تعیین می‌شود» [۹]

به واقع ماده ۱۳ اخیر، دست قاضی را در تشخیص ارزش دلایل الکترونیکی ساده در مقایسه با سایر دلایل باز گذاشته است. اما در خصوص دلایل الکترونیکی مطمئن، همان‌طور که گفته شد، قانون تجارت الکترونیکی در ماده ۱۴ خود آن را در حکم اسناد معتبر و قابل استناد دانسته و در ماده ۱۵ انکار و تردید را نسبت به آن مسموع ندانسته است. به عبارت دیگر، مقنن از پیش، ارزش این‌گونه دلایل را در مقایسه با اسناد عادی تعیین کرده است. اما چنانچه ادله الکترونیکی با اسناد رسمی کاغذی در تعارض قرار گیرد، با توجه به سکوت قانون تجارت الکترونیکی، حل این تعارض مسلماً با قاضی است که با توجه به اختیاری که در کشف حقیقت دارد، در این خصوص تصمیم‌گیری کند و دلیلی که به حقیقت نزدیک‌تر است.

نتیجه‌گیری

با تصویب قانون تجارت الکترونیکی و تعیین چارچوب‌های حقوقی امضای الکترونیکی، یک گام اساسی برای عملی ساختن مبادلات الکترونیکی و پیوستن به تجارت الکترونیکی برداشته شده است. با این حال از یک سو مقررات راجع‌به امضای

الکترونیکی دارای ایراداتی است که باید هر چه زودتر برطرف شود و از سوی دیگر آیین‌نامه‌های مرتبط با امضای الکرونیکی از جمله ایجاد دفاتر خدمات صدور گواهی الکترونیکی آماده شود. بدیهی است وجود زیرساخت‌های حقوقی به تنهایی کافی نیست بلکه زیرساخت‌های فنی تجارت الکترونیکی باید هر چه زودتر آماده شود تا امکان پیوستن به دنیای تجارت الکترونیکی فراهم شود. این زیرساخت‌ها باید به گونه‌ای باشد که نه تنها در داخل کشور مراجع قضایی با اطمینان از امنیت داده‌های مرتبط با امضای الکترونیکی، تمامیت و تک و منحصر بودن آنها و هویت امضاءکننده امضای الکترونیکی را در حکم سند رسمی بپذیرند بلکه در عرصهٔ بین‌المللی نیز دفاتر صدور گواهی خدمات الکترونیکی ایران به رسمیت شناخته شوند تا ایران به قافله تجارت الکترونیک که حرکت خود را مدتهاست آغاز کرده بپیوندد.

منابع

[1] Heut; "La modification du droit sous l'influence de l'informatique"; *Jcp*, no. 13781, 1982.

[2] Gautier" P.Y. et Linant de Bellefonds, Xavier, "De l'écrit electronique et des signatures quis'y attachent", Jcp, ed. G., no. 1236, 2000.

[۳] *گزارش توجیهی پیش‌نویس قانون تجارت الکترونیکی*، مرکز ملی شماره‌گذاری کالا و خدمات ایران وابسته به مؤسسه مطالعات و پژوهش‌های بازرگانی، پاییز ۸۰.

[4] Huet, J; "Vers une consecration de la preuve et de la signature éléctronique: Dalloz, doctr. no. 6, 2000.

[5] Caprioli, Eric; "La loi francaise sur la preuve et la signature éléctronique dans la perspective européénne"; *J.C.P*. éd, no. 2. Gen. 2000.

[۶] جعفری لنگرودی، جعفر؛ *ترمینولوژی حقوق*؛ چ ۵، تهران: گنج دانش، ۱۳۷۰.

[7] Cornu. G.; *Vocabulaire juridique*, Association Henri Captitan, puf, 2000.

[8] *Lamy droit de l'informatique et des réseaux*, éd. lamy, p. 1674, no. 2976, 2002.

[۹] قانون تجارت الکترونیکی مصوب ۸۲/۱۰/۲۹ مجلس شورای اسلامی

[۱۰] قاجار، سیامک؛ «تجارت الکترونیک و جرائم مرتبط با آن»؛ *مجموعه مقالات اولین همایش تخصصی بررسی جرائم رایانه‌ای*، تهران: معاون اگاهی ناجار، ۱۳۸۰.

[۱۱] گلچیان نیک، فرشته؛ «تحقق بیع بین‌المللی در تجارت الکترونیک» *رساله دوره کارشناسی ارشد دانشکده حقوق و علوم سیاسی دانشگاه علامه طباطبایی*.

[12] Jacques, L; Le décret no. 2001-272 du 30 mars 2001 relatif à la signature éléctronique, *J.c.p*, éd. Gén. 2001.

[۱۳] جعفرپور، ناهید؛ «آیین دادرسی جرایم کامپیوتری» ، *خبرنامه انفورماتیک*، ش ۸۴ (آبان ۸۱)

[۱۴] کاتوزیان، ناصر؛ اثبات و دلیل اثبات؛ ج ۱، تهران: نشر میزان، ۱۳۸۰.

[15] Code Civil, Dalloz, éd. 2003.

[16] Terre, Francois; *introduction générale au droit*, Dalloz; 5 ed, 2000.

☑ عنوان: تحلیل حقوقی جنبه‌هایی از پرداخت‌های الکترونیکی

☑ نویسنده: دکتر امیر صادقی نشاط (عضو هیأت علمی دانشگاه تهران)

مقدمه

پول در جهت تسهیل معاملات ابداع شد و در طول زمان نیز صورت‌های گوناگون به خود گرفت تا آنکه پس از طی دوران سکه‌های با ارزش ذاتی، به سکه‌های امروزه و اسکناس‌های رایج که ارزش خود را از پشتوانه دریافت می‌کنند منجر گردید.

از آنجا که حجم و ارزش این پولها، نقشی اساسی در نظام اقتصادی کشورها و سلامت بازار داشته‌اند، همواره ضرب سکه‌ها و انتشار اسکناس‌ها جزء وظایف حکومتی قرار داشته و به عهدهٔ سازمانی دولتی محول گردیده است.

در ایران نیز، طبق قانون نظام پولی و بانکی کشور، این کار جزء وظایف بانک مرکزی جمهوری اسلامی قرار گرفته و تنها سکه‌ها و اسکناس‌هایی دارای اعتبار شناخته شده‌اند که مطابق مقررات مربوط توسط بانک مزبور ضرب، چاپ و منتشر گردیده باشند.

امروزه با توسعهٔ فناوری اطلاعات و طراحی نرم افزارها و سیستم‌های پیشرفته که در اختیار بانک‌ها و مؤسسات مالی قرار گرفته، روش‌ها و ابزارهای جدیدی برای پرداخت به صورت الکترونیک به وجود آمده که بعضاً در مفهوم و یا نحوهٔ کاربرد آنچه که قبلاً وجود داشته است، تغییراتی را موجب شده است. پولهای دیجیتالی، چک الکترونیک و کارت‌های پرداخت هوشمند و غیر هوشمند، از جملهٔ این ابزارها و روش‌ها و با عنوان کلی «پرداخت الکترونیک» قرار دارند که در ادامه به بحث در خصوص پاره‌ای از جنبه‌های حقوقی آنها خواهیم پرداخت.

الف ـ پول الکترونیک (e-money)

با حضور و دخالت غیر قابل تفکیک بانکها در اقتصاد کشورها و جریان مبادلات بین تجار، و تجار با مصرف کنندگان، مبادلات پولی در حجمهای زیاد آسان گردید، به طوری که با استفاده از شبکه بانکی می‌توان حتی بدون آنکه عملاً پولی معادل بهای معاملات در شعبهٔ بانک وجود داشته باشد مبالغ هنگفتی را نقل و انتقال داد، تنها حسابی بدهکار می‌شود و حسابی دیگر بستانکار.

بدیهی است که می‌توان خدمات مزبور را دستی نیز انجام داد همانطور که تا همین سالهای اخیر، تمام بانکداری به روش دستی انجام می‌گرفت و حداکثر برخی امور نیز به کمک تلفن و سپس تلکس و فاکس هماهنگ می‌شد ولی با ظهور و رواج کامپیوتر و پیدایش سخت افزارهایی با حجم نسبتاً کم ولی با حجم حافظه و سرعت پردازش بسیار زیاد در سطوح Mainframe ها و PC ها، و مخابرات با حجم و سرعت زیاد، بانکداری جهش زیادی یافت و خدمات متنوع‌تری در امور سرمایه گذاری، نقل و انتقال پولها در تجارت میسر گشت.

با توجه به اینکه در بانکها، که تحت کنترل و نظارت بانک مرکزی قرار دارند، حسابها به صورت الکترونیک نگهداری می‌شوند وضمناً نقل و انتقال وجوه بین حساب اشخاص نیز با سرعت زیاد و ایمن قابل انجام است، خود به خود نیاز به پولهای مسکوک و اسکناس کاهش می‌یابد و عملاً بانک مرکزی نیز مقدار کمتری اسکناس منتشر می‌نماید. به عبارت دیگر، در واقع ضمن آنکه مقدار پول کاهش نمی‌یابد نیاز جامعه به پولهای مسکوک یا اسکناس در حد زیادی رفع می‌شود.

در این موارد بدون آنکه در حاکمیت قانون پولی و بانکی و انحصار اعتبار پول به صورتهای رایج لطمه بخورد تحلیل حقوقی این واقعیت آن است که وقتی شخصی پولی نزد یک بانک دارد، از بانک طلبکار است و هنگامی که وجوهی از طریق آن بانک از فرد مزبور و دیگری نقل و انتقال می یابد در واقع بانک به جای بدهکاری به طرف اول، به طرف دوم بدهکار می گردد. بدین ترتیب عمدتاً فقط آن مقدار از پول که توسط مصرف کنندگان در بازار خرج می‌شود و خارج از سیستم بانکی قرار دارد به صورت اسکناس یا سکه می‌باشد.

حال اگر این روند را توسعه دهیم به پولی می‌رسیم که اخیراً ابداع شده که پول الکترونیک یا پرداخت نقدی الکترونیک(e-cash) خوانده می‌شود. این پول با آنکه ممکن است به صورت سکه و یا اسکناس باشد، ولی توسط دولت ضرب یا منتشر نمی‌شود. در این نوع پول، شخص می تواند از بانکی که نزد آن پول رسمی سپرده است بخواهد مبلغی پول الکترونیک به وی اختصاص دهد. این پولها به صورت سکه یا اسکناسهایی با طرحها و ارزشهای انتخابی خواهند بود، مثلاً سکه های یک، دوازده ویک میلیون ریالی.

در این سیستم پولی سه طرف وجود دارد: بانک یا مؤسسه مالی، کاربر یا مشتری و شخص تاجر. ابتدا مشتری حسابی نزد بانک افتتاح می‌کند که موجودی آن از طریق پرداخت نقدی یا اعتبار تأمین می‌شود. سپس مشتری بر اساس موجودی حساب خود سفارش مقداری پول را با ارزشهای انتخابی می‌دهد و پس از آنکه پولها در رایانهٔ وی دریافت شد در محلی همانند یک کیف پول نگهداری می‌شود. از طرف دیگر، تاجر یعنی عرضه کنندهٔ کالا یا خدمات نیز حسابی نزد بانک مزبور خاص این روش افتتاح می‌نماید. وقتی معامله‌ای بین تاجر و مشتری صورت می‌گیرد، مقداری از پول‌های موجود نزد مشتری برای تاجر ارسال می‌شود. در این مرحله سیستم پیامی روی مونیتور می‌فرستد که حکایت از انجام معامله دارد.

به منظور ایمنی این سیستم پرداخت، اولاً شماره‌های سکه‌ها در سیستم کنترل می‌شود تا از بروز تقلب و کپی شدن آنها جلوگیری شود، و ثانیاً پیام‌ها به همراه امضای الکترونیک مشتری متضمن دو کلید دیجیتالی مبادله می‌شوند، و ثالثاً حتی بانک صادر کننده از محتوای پیام‌های فیمابین مشتری و فروشنده و کم و کیف مورد معامله بی‌اطلاع می‌ماند زیرا پیام‌ها درون پاکت‌های دیجیتالی مبادله می‌گردند و به این طریق حریم خصوصی افراد محفوظ باقی می‌ماند و همین امتیاز سبب شده است مردم این روش پرداخت را بر روش استفاده از کارت‌های اعتباری ترجیح دهند.

از جملهٔ نکته‌های دیگر قابل طرح در این نوع پول یا روش پرداخت موارد زیر است:

۱ـ آیا اینگونه سکه‌ها که حتی شکل و مقدار آن مشابه سکه‌های رسمی نیست، پول تلقی می‌شوند؟

پاسخ این است که تا به آنجا که به ملاحظات اقتصادی مربوط می‌شود ظاهراً این سکه‌ها پول محسوب می‌شوند و دارای همان نقش پول‌های رسمی هستند، و بلکه از آنجا که نقل و انتقال و در نتیجه سرعت و سهولت کاربری آنها بیشتر است، خاصیت پولی بیشتری از سکه‌ها و اسکناس‌های رسمی دارند، به همین جهت است که عرفاً پول محسوب می‌شوند.

ولی نظر به اینکه فعلاً قوانین کشورها از جمله قانون پولی و بانکی جمهوری اسلامی ایران پول را تنها منحصر به سکه‌ها و اسکناس‌هایی می دانند که توسط بانک مرکزی و مطابق مقررات و تشریفات خاص صادر شوند، قانوناً نمی‌توان اینگونه سکه‌ها را پول محسوب نمود.

نتیجه این تحلیل آن خواهد شد که وقتی اینگونه سکه‌ها از رایانهٔ مشتری به رایانهٔ خریدار ارسال می‌شود مادام که نزد بانک صادرکننده که نگهدارندهٔ پولهای رسمی معادل آن است نرسیده و به حساب فروشنده منظور نگردیده است، بهای قرارداد پرداخت شده محسوب نمی‌شود. زیرا اینگونه سکه‌ها فی نفسه پول نیستند و مادام که معادل آنها از پول رسمی به حساب فروشنده منظور نشده باشد، پرداخت بها انجام نشده است.

بر این اساس، چنانچه در فاصلهٔ ارسال این سکه‌ها تا طلبکار شدن حساب فروشنده به پول رسمی اتفاقی بیفتد، مثلاً سرقت شود، به طوری که حساب فروشنده عملاً پول رسمی را دریافت نکند، اصل برآن است که سرقت از مال مشتری انجام شده است، مگر آنکه دلیل دیگری موجود باشد که نشان دهد فروشنده ریسک مراحل بعد از رایانهٔ مشتری را قبول کرده است که دراین صورت نیزاز این باب که فروشنده مسؤولیت و خطر مراحل بعد از انتقال سکه‌های غیر رسمی را پذیرفته است، و نه از جهت اعتبار پول‌ها، دیگر نمی تواند ادعایی علیه مشتری بنماید. ولی اگر بعداً کشف شود که سکه‌های مزبور در اثر اشتباه یا خرابکاری رایانه‌ای از ابتدا بدون پشتوانه پول‌های رسمی از سوی بانک تولید شده‌اند در آن صورت هنوز مشتری بدهکار بهای قرارداد منعقده خواهد بود.

اما این که آیا توجیهی وجود دارد که قانونگذاران اینگونه پول‌های دیجیتالی را نیز به عنوان پول رایج و رسمی بپذیرند؟

به نظر می‌رسد آنچه از نظر قانون در این زمینه جنبهٔ اصلی دارد، «ارزش» پول رسمی است نه شکل آن. بنابراین اگر روزی فناوری اطلاعات به نحو گسترده و مطمئن اجازه دهد مردم براساس ارزش واحد رسمی پول، مثلاً ریال، دینار یا دلار، پولهایی با سلیقه خود طراحی و فی مابین خود در شبکهٔ رایانه‌ای مبادله کنند ولی حساب آنها در واقع از طریق سیستم بانکی تحت کنترل و نظارت بانک مرکزی قرار داشته باشد، اشکالی پیش نخواهد آمد. بنابراین لازم نیست سکهٔ خاص یا اسکناسی با طرح دولتی تولید و در اختیار عموم قرار گیرد تا ارزش پولی پیدا کند.

مطلبی که مناسب است در پایان این مبحث اضافه شود این است که گاه تحت عنوان پول دیجیتالی، مشتری مقداری از موجودی حساب اصلی خود در بانک به کارت خویش که دارای امکانات هوشمندانه است واریز می‌کند (کیف پول الکترونیک e-purse) و همانند کارت تلفن، با استفادهٔ از آن به خرید کالا و خدمات مورد نیاز تا صفر شدن موجودی کارت می‌پردازد. در اینجا بحث پول الکترونیک به شکل قبل مطرح نیست بلکه تنها حساب پول‌های مبادله شده بین رایانهٔ مشتری، تاجر و مؤسسه مالی صادرکنندهٔ کارت و دریافت کنندهٔ وجه، با همان پول رسمی نگهداری می‌شود و مسأله پول جدید مطرح نیست.

در اینجا اگر واقعاً همهٔ تراکنشها از صادرکننده تا مشتری و از مشتری تا تاجر صحیح انجام شود عمل پرداخت و دریافت وجه انجام شده است ولی اگر مثلاً مشتری به اندازه ای که به کارت خود منتقل نموده نزد بانک خود موجودی یا اعتبار نداشته و به اشتباه یا عملیات مجرمانه و ایجاد اختلال یا دستکاری در سیستم، کارت مشتری از مبلغی موجودی پر و سپس با آن معامله شده باشد در آن صورت اگر حساب‌های بانک متناسب با مبلغ مزبور بستانکار شده باشد در واقع پول سرقت گردیده و هر حکمی که معاملهٔ با اموال مسروقه دارد همان حکم نیز در اینجا جاری خواهد شد. به عبارت دیگر مالک پول، بانک بوده و معامله تا توسط آن تنفیذ نشود (که معمولاً نمی‌شود) صحیح نخواهد بود. ولی اگر در حساب‌های بانکی نیز هیچ اثری از نقل و انتقال

وجوه فی‌مابین بانک و مشتری وجود نداشته باشد در این صورت اصلاً پولی بین خریدار و فروشنده مبادله نگردیده و معامله از اصل باطل است، علاوه بر این از نظر کیفری نیز عمل مشتری قابل بررسی و توصیف است که آیا در حکم جعل یا کلاهبرداری است یا سرقت اموال دیگران با تمهیدات ویژه‌ای که در تراکنشها انجام داده است؟ یا آنکه مرتکب تعدد جرم جعل و کلاهبرداری یا سرقت شده است؟ البته این مقاله در مقام بررسی این جوانب از موضوع نیست و می‌تواند در جای خود مورد بررسی قرار گیرد.

ب ـ چک الکترونیک

اصولاً اسناد تجاری به ویژه چک، به عنوان وسیله‌ای در مبادلات تجاری ابداع شدند تا بدون آنکه ذاتاً اعتبار پول داشته باشند طرفین را از حمل و تحویل و تحول سکه یا اسکناس در حجم زیاد بی‌نیاز نمایند.

حکومت‌ها نیز با وضع قوانین در حمایت از قابلیت انتقال آنها و نیز عدم قابلیت استناد به ایرادهای فی‌ما بین مسؤولین در برابر دارنده اسناد مزبور، سرعت و اعتبار آنها را در جریان تجاری افزایش دادند.

همانطور که پیش بینی می‌شد، اینک با توسعه فناوری اطلاعات امکان صدور چک الکترونیک (و البته سایر اسناد تجاری ولو آنکه هنوز معمول نیست) به وجود آمده و برخی بانک‌ها در کشورهای پیشرفته در این زمینه امکان صدور چک را به آن صورت در اختیار مشتریان خود قرار داده‌اند.

در این روش، بانک کارت هوشمندی را که متضمن برنامه‌ای است به مشتری می‌دهد که وی می‌تواند مندرجات چک را به صورت رمز درآورد و علاوه بر این دیسکتی نیز در اختیار او می‌گذارد که در آن برنامه صدور چک وجود دارد. تعداد چکها می‌تواند نامحدود باشد.

وقتی برنامه فعال می‌شود فرم چک روی صفحه نمایش ظاهر و توسط مشتری تکمیل و با کلید اختصاصی مشتری امضاء و به عبارت دیگر به صورت رمز درمی‌آید. وقتی چک تکمیل و برای دریافت کننده ارسال می‌گردد، شخص اخیر به وسیله کلید عمومی صادرکننده آنرا به صورت خوانا در آورده و سپس برای بانک خود جهت وصول ارسال می‌نماید. بانک تأیید صدور را از مرکز گواهی امضای الکترونیک (Center of Authority) دریافت می‌کند (البته این یک اقدام احتیاطی تکمیلی است) و سپس همانند سایر چکها آنرا جهت وصول به جریان می‌اندازد که یا نقد خواهد شد یا برگشت خواهد گردید.

کلر کردن این چکها نیز می‌تواند در صورتی که هر دو بانک صادرکننده و دریافت کننده دارای امکانات الکترونیک به این منظور باشند به سرعت و به همین روش انجام پذیرد.

نکته‌ای که از نظر قانون تجارت و قانون صدور چک قابلیت بررسی دارد آن است که در قانون تجارت ازچک به عنوان «نوشته» تعبیر شده در حالی که ممکن است اشکال شود که آنچه در عالم الکترونیک اتفاق می‌افتد اصلاً به صورت نوشته نیست و نوشتن تنها در مرحلهٔ ظاهری تنظیم و ابتدای جریان چک الکترونیک مطرح است به طوری که روی صفحه کلید و نهایتاً صفحه نمایش به صورت عبارات و ارقام شکل می‌بندد، ولی آنچه در واقع وجود دارد جز اختلاف ولتاژهای درون رایانه و جریانات الکترونیک نیست و البته با این امکان که مجدداً به صورت حروف و ارقام ظاهر و روی کاغذ چاپ گردد.

ممکن است برای رفع این اشکال گفته شود که درست است که قطعاً در قدیم و آنگاه که قانونگذاران چک را به عنوان نوشته تعبیر کرده‌اند نظرشان به چک الکترونیک نبوده است ولی مسلماً در نوع و جنس حامل چک نیز تا آنجا که به ماهیت چک مربوط می‌شود نظر خاص نداشته‌اند. مثلاً کاملاً امکان داشته است که چک به جای آنکه روی کاغذ صادر شود روی

پوست حیوانات و یا تکه‌های چوب و غیره نیز صادر گردد. و نیز قانون نظر به این ندارد که چه جریانات و مقدماتی باید طی گردد تا آنکه چک صادر شود. آنچه برای قانون مهم است آن است که سند مزبور بتواند عنوان داشته باشد و ضمناً با امضای آن قابلیت انتساب به صادرکننده را نیز پیدا نماید. حال اگر این جریان به طریق الکترونیک نیز باشد برای قانونگذار تفاوتی نخواهد کرد. چک در مبدأ صدور به صورت نوشته است در مدت ارسال به صورت غیر نوشته و در نهایت نیز به صورت نوشته روی صفحه مونیتور ظاهر می‌شود و ممکن است به همان صورت نیز چاپ گردد. علاوه براین، مطابق ماده ۶ قانون تجارت الکترونیکی مصوب ۱۳۸۲، «هرگاه وجود یک نوشته از نظر قانون لازم باشد، «داده پیام» در حکم نوشته است مگر در موارد زیر: الف ـ اسناد مالکیت اموال غیر منقول، ب ـ فروش مواد دارویی به مصرف کننده نهایی، ج ـ اعلام، اخطار، هشدار و یا عبارت مشابهی که ..... » اگرچه این قانون نسبت به قانون چک عام است ولی چون مؤخر است می تواند در آن مورد نیزقابلیت استناد داشته باشد به ویژه آنکه در بخش استسنائات سخنی از اسناد تجاری به میان نیامده است.

درخصوص امضای این گونه چکها نیز نکتهٔ دیگری قابل طرح است. در چک، برخلاف سفته یا برات که صدور یا مهر نیز تجویز شده، تنها امضای صادرکننده را ضروری شمرده است. حال سؤال این است که آیا امضاهای الکترونیک خصوصاً در شکل زوج کلیدهای عمومی و خصوصی واقعاً در ردیف مهر هستند یا امضا؟ یا اینکه ماهیت سومی دارند با خواص اضافه بر آنچه مهر یا امضای سنتی داشته اند؟ البته موضوع این مقاله به طور خاص امضای الکترونیک نیست و در اینجا به اختصار و جهت حل مسأ لهٔ اخیر اشاراتی به این مطلب می‌شود.

به هر حال، گرچه این گونه به اصطلاح امضائات به ویژه اگر با تأیید از سوی مرجع گواهی آن نیز همراه باشد، علاوه برآنکه انتساب یک سند را به صادرکننده روشن می‌کند خاصیت اضافی نیز دارند و آن عبارت از این است که در خصوص عدم تغییرات در متن پس از امضاء نیز اطمینان می‌دهند، ولی در مقام مقایسه بیشتر با مهر مشابهت دارد تا امضا، ضمن آنکه به لحاظ ماهیت اساساً با هر دوی آنها متفاوت است. امضای الکترونیک به صورت دو کلید عمومی و خصوصی، جز دو سری فرمول‌های ریاضی نیست که از سوی مراجع تأیید امضاء در اختیار اشخاص قرار می‌گیرند به طوری که هرگاه به کمک یکی از آنها متنی به صورت رمز درآید به کمک دیگری رمزگشایی خواهد شد. کلید عمومی در اختیار همگان است درحالی که کلید دیگر تنها در اختیار صاحب امضاء قرار دارد.

بدین ترتیب گرچه این دو کلید که ماهیتی ریاضی دارند و در عرف نام امضاء یافته‌اند و قانونگذار نیز در قانون تجارت الکترونیک به تبع عرف آنها را امضاء نامیده است، از آنجا که توسط شخصی ثالث (مرجع صدور گواهی .C.A) تولید و به اشخاص اختصاص داده می‌شوند و اشخاص فقط آنها را به شکلی که هستند مورد استفاده قرار می‌دهند، در تحلیل حقوقی در ردیف مهر قرار می‌گیرند. حال اگر چنین است آیا می‌توان چک را با آنها صادر نمود؟

پاسخ این است که با تصویب قانون تجارت الکترونیک به ویژه مواد ۱۲ تا ۱۶ باید گفت حتی اگر امضای الکترونیک در ردیف مهر نیز باشد، قانون تجارت و قانون صدور چک در این خصوص نسخ شده‌اند و در واقع چکها می‌توانند یا با امضاء به مفهوم سنتی و یا با امضای الکترونیک (ولو آنکه واقعاً مهر الکترونیکی باید تلقی شود) صادر گردند.

نکته دیگری که می توان از نظر حرفهٔ حقوقی در زمینه صدور چک و ایمن سازی مبادلات تجاری متذکر شد این است که می‌توان پیشنهادی به شرکت‌های فنی و مؤسسات مالی ارائه داد که نرم افزارهایی را طراحی و به مرحله اجرا درآورند که ضمن آنکه امکان صدور چک را به طریق الکترونیک در اختیار مشتریان قرار دهند این قابلیت را نیز داشته باشند که به صورت به

هنگام، کنترل آن از لحاظ وجود محل نیز ممکن باشد به طوریکه اگر چکی فاقد محل یا کسر موجودی باشد از همان ابتدا، امکان صدور آن به طریق الکترونیک وجود نداشته باشد. علاوه براین باز این امکان وجود دارد که پیشنهاد شود نرم افزار مزبور را طوری طراحی کنند که پس از صدور، معادل وجه آن در حساب مشتری بلوکه و به همان چک اختصاص داده شود و به عبارت دیگر، «چک تأیید» شده که در قانون صدور چک پیش‌بینی شده، به این طریق امکان اجرایی سهل و سریع پیدا می‌کند و چک‌ها نه تنها به لحاظ صحت صدور بلکه به لحاظ کنترل موجودی و تأیید آن نیز اطمینان بخش تر خواهند گردید.

نکتهٔ دیگری نیز که می‌توان از لحاظ حقوقی ـ اجرائی اضافه نمود آن است که با امکان صدور چک الکترونیک به صورت به هنگام، دیگر در واقع نیاز به سندی به نام چک نخواهد بود زیرا اگر بتوان به صورت به هنگام حسابها را از طریق سیستم‌های خاص بانکداری بدهکار و بستانکار نمود در آن صورت صدور حواله الکترونیک کافی خواهد بود و نیازی به چک به عنوان یک سند تجاری و با احکام خاص قدیمی به عنوان وسیلهٔ پرداخت نخواهد بود.

☑ عنوان: لحظه انعقاد قرارداد از طریق واسطه‌های الکترونیک

(موضع قانون نمونه آنسیترال و قانون تجارت الکترونیک ایران)

☑ نویسنده: آقای فیضی چکاپ

(عضو هیأت علمی دانشکده حقوق و علوم سیاسی دانشگاه علامه طباطبایی)

مقدمه:

استفاده از تلفن، تلکس و فاکس در معاملات تجاری ملی یا بین‌المللی از مدتها پیش معمول گردیده است. و دیر زمانی است که بازرگانان به کمک این وسایل بدون حضور در یک مجلس مبادرت به انعقاد قراردادهای بازرگانی از راه دور می‌نمایند. اما هیچگاه فضای مجازی الکترونیک به نحوی که امروزه شاهد آن هستیم در روابط واقعی طرفین قراردادهای بازرگانی داخلی و منطقه‌ای و بین‌المللی تأثیر نداشته است.

استفاده از واسطه‌های الکترونیک و پدیدهٔ سحر آمیز IT و EDI، وضعیت و موقعیت بسیاری از عناصر قراردادهای خرید و فروش کالا و خدمات را در معرض ابهام و اشکال قرار داده و مسائل حقوقی زیادی را مطرح نموده است. که دست اندرکاران امر، اقتصاددانان، بازرگانان و حقوقدانان نمی‌توانند نسبت به آنها بی‌تفاوت باشند. می‌توان گفت بدون تعیین تکلیف و شفاف‌سازی این مسائل تنظیم روابط و تعیین حقوق و تکالیف اشخـــاص غیر ممکن است.

به عنوان مثال: هر یک از روشهای خرید و فروش کالا، اعم از B to B،B to C، حراج کالا بر روی شبکه، توزیع اینترنتی کالا و خدمات، بانکداری الکترونیکی و .... مبتنی بر یک یا چند قرارداد هستند که مبنای ایجاد تعهد برای طرفین قرارداد را تشکیل می‌دهند[1]. با توجه به اینکه در قراردادهای منعقده از طریق واسطه‌های الکترونیک اصولا" طرفین عقد در یک مکان قرار ندارند و قرارداد از راه دور منعقد می‌شود. ممکن است ایجاب و قبولی که بین فروشنده و خریدار مبادله می‌گردد نیز تقارن و توالی زمانی نداشته باشد. این وضعیت حداقل دو سئوال ایجاد می‌کند.

۱- لحظه وقوع عقد چه زمانی است؟

۲- مکان وقوع عقد کجا است؟

پاسخ این سئوالات تاثیر اساسی در سرنوشت و آثار قرارداد دارد. و ممکن است حقوق و تکالیف طرفین قرارداد را دگرگون سازد. زیرا اعتبار و یا بطلان عقد، دادگاه حاکم بر قرارداد، قانون حاکم بر قرارداد، شروع تعهدات طرفین، دوره گارانتی و حتی مبلغ قرارداد و امثال آن تماما" به زمان و مکان وقوع عقد بستگی دارد. با توجه به اینکه قانون نمونه آنسیترال و همچنین قانون

1- Le commerce électronique: un nouveau mode de contracter? Actes du colloque par la Faculté de droit de l` Université de Liège (Unité de Droit privé) et la Conférence libre du jeune Barreau de Liége le 19 avril 2001 A.S.B.L. Editions du Jeune Barreau de Liège 2001, pp 51 et s.

تجارت الکترونیک ایران قواعد ماهوی نیستند به مسئله زمان و مکان وقوع قرارداد و آثار حقوقی آن توجه ننموده‌اند و آنرا به قواعد عمومی واگذار نموده‌اند. برعکس زمان ارسال و دریافت داده پیام و مکان ارسال و دریافت داده پیام را مورد توجه قرار داده‌اند. بنابراین برای تعیین زمان و مکان قراردادهای منعقده از طریق واسطه‌های الکترونیک علاوه بر مقررات ناظر به تجارت الکترونیک باید به قواعد عمومی قراردادها نیز توجه نمود.

در این مقاله سعی شده است با توجه به حقوق کشورهای مختلف و کنوانسیون وین ۱۹۸۰ ناظر به بیع بین‌المللی کالا از یک سو، و قانون نمونه آنسیترال در مورد تجارت الکترونیک (۱۹۹۶) و قانون تجارت الکترونیک ایران (۱۳۸۲) از سوی دیگر، بررسی و معلوم شود که در قراردادهای راه دور که از طریق واسطه‌های الکترونیک منعقد می‌شوند، تلاقی اراده طرفین عقد چگونه منجر به وقوع قرارداد می‌گردد. و لحظه وقوع عقد چه زمانی است و مکان وقوع عقد کجا است؟ تا تجار و بازرگانان محترم که از طریق تجارت الکترونیک اقدام می‌نمایند. از آثار اقدامات on line خود برای انعقاد قرارداد مطلع باشند.

بدین منظور ابتدا مسئله چگونگی تلاقی اراده طرفین قرارداد در فضای الکترونیک را بررسی می‌نماییم (مبحث نخست). و برای درک صحیح مفهوم ایجاب و قبول قبل از هر چیز این موضوع را با توجه به حقوق ایران و برخی کشورهای اروپایی مورد بررسی قرار داده (بند الف) سپس ضمن بررسی انواع ایجاب، بین ایجاب و دعوت به ایجاب تفکیک قائل خواهیم شد (بند ب).

با فراغت از مباحث فوق‌الذکر به منظور تعیین زمان و مکان انعقاد قرارداد از طریق واسطه‌های الکترونیک (مبحث دوم). ابتدا اهمیت و آثار تعیین زمان و مکان در این نوع قراردادها را اختصارا" احصاء نموده (بند الف) و سپس مکان و زمان وقوع عقد در قراردادهای منعقده از راه دور را مطالعه می‌نماییم (بند ب). و در خاتمه برای تعیین زمان و مکان وقوع قرارداد از طریق واسطه‌های الکترونیک مسئله ارسال و دریافت پیام‌های الکترونیک را با توجه به ماده ۱۵ قانون نمونه آنسیترال و مواد ۲۶ الی ۳۰ قانون تجارت الکترونیک ایران مورد بررسی قرار می‌دهیم (بند ج).

مبحث نخست: تلاقی اراده طرفین قرارداد در فضای الکترونیک.

هر قراردادی با ایجاب و قبول (لفظی یا عملی) که مبین تلاقی اراده طرفین قرارداد است منعقد می‌گردد. لذا وقتی سخن از برخورد و همنوائی اراده‌ها می‌شود ایجاب و قبول و انواع آن به ذهن متبادر می‌شود. ابتدا مفهوم ایجاب و قبول را بررسی نموده (الف) و سپس بین ایجاب و دعوت به ایجاب تفکیک قائل می‌شویم تا عملاً فرق ایجاب به شخص معین و ایجاب به عموم را نیز مطالعه نموده باشیم.(ب)

الف) مفهوم ایجاب و قبول:

قانون مدنی ایران ایجاب را تعریف نکرده است. قانون تجارت الکترونیک ما که با تکیه بر قانون نمونه آنسیترال[۲] وضع گردیده نیز اشاره‌ای به مفهوم ایجاب و قبول ننموده است. البته در ماده ۱۹ پیش نویس قانون تجارت الکترونیک ایران به تبعیت از ماده ۱۱ قانون نمونه آنسیترال بدون تعریف از ایجاب، قید شده بود که: ((ایجاب، قبول و اعلام اراده در ارتباط بین اصل ساز و مخاطب به وسیله داده پیام بیان می‌شود...))[۳]. این ماده در شور دوم مجلس حذف گردید. برخی از نویسندگان حقوق مدنی

۲- loi type de la CNUDCI sur le commerce électronique (1996)

۳- متن ماده ۱۱ قانون نمونه آنسیترال به شرح زیر است:

گفته‌اند ایجاب ((در اصطلاح حقوق مدنی رضای عاقد است که حالت فعلی (تاثیری) دارد، در برابر رضای طرف که جنبه انفعالی دارد و آنرا قبول گویند...))[۴]. در حقوق برخی کشورهای اروپایی ایجاب عبارت است از ارسال پیام مشخص، دقیق و قطعی به وسیله ایجاب کننده برای مخاطب مبنی بر انعقاد عقد با وی به نحوی که فقط قبولی مخاطب برای تحقق قرارداد کافی باشد[۵].
مفاد ایجاب باید بر روی نکات اساسی قرارداد و عناصری که در هر مورد خاص مورد توافق قطعی طرفین است متمرکز باشد.
بند ۱ ماده ۱۴ کنوانسیون وین (۱۹۸۰) که ناظر به فروش‌های بین‌المللی کالا است در این زمینه مقرر نموده است که: ((پیشنهاد انعقاد قرارداد خطاب به یک یا چند شخص معین در صورتی ایجاب محسوب می‌شود که به اندازه کافی مشخص بوده و دال بر قصد التزام ایجاب کننده در صورت قبول باشد. پیشنهاد در صورتی به اندازه کافی مشخص است که کالا را معین نموده و به نحو صریح یا ضمنی مقدار و ثمن را نیز معین یا ضوابطی جهت تعیین آن دو مقرر نماید.))
مطابق قواعد حاکم بر تجارت الکترونیک چنانچه یک ایجاب با رعایت شرائط لازم[۶] در شبکه‌های اینترنتی و فضای الکترونیک و درگالری‌های مجازی ارائه شود از نظر حقوقی می‌تواند اثر ایجاب در فضای واقعی و معمولی را دارا باشد. همین حکم در ذیل ماده ۱۱ قانون نمونه آنسیترال به این نحو بیان شده است. ((...هنگامی که برای انعقاد قرارداد از داده پیام استفاده می‌شود، اعتبار یا قدرت اجرائی قرارداد صرفا" به این دلیل که از داده پیام استفاده شده از بین نمی‌رود.)) هر چند که مضمون این ماده در ماده ۱۹ پیش نویس قانون تجارت الکترونیک ایران درج شده بود و بعدا" حذف گردیده است. اما از آنجا که اساس قانون تجارت الکترونیک مبتنی بر تبادل داده پیام است و با توجه به سایر مواد قانون مزبور بدیهی است که این حکم مورد قبول قانون تجارت الکترونیک ایران نیز می‌باشد.

ب) تفکیک بین ایجاب و دعوت به ایجاب:

مطلب قابل توجه این است که مفهوم ایجاب در نظام حقوقی کشورهای مختلف یکسان نیست، گاه پیشنهاد فروش ارائه شده به شکل معینی در برخی از کشورها ایجاب تلقی می‌شود. در نتیجه به محض قبول مخاطب قرارداد منعقد شده تلقی می گردد. همان پیشنهاد مطابق حقوق کشور دیگر ممکن است ایجاب تلقی نگردد. بلکه نوعی دعوت از دیگران برای ارائه پیشنهاد (ایجاب) باشد. در این صورت پس از اینکه مخاطب به دعوت مزبور پاسخ بدهد و پیشنهاد خود را عرضه کند، نوبت به فروشنده می‌رسد که تصمیم بگیرد آیا پاسخ مثبت بدهد یا خیر؟ وی حق دارد ایجاب واصله را قبول کند یا آنرا رد نماید. معمولاً چنانچه

در چهار چوب انعقاد قراردادهاایجاب و قبول می تواند از طریق داده پیام بیان شود, مگر آنکه طرفین به نحو دیگری توافق نموده باشند. هنگامیکه برای انعقاد قرارداد از داده پیام استفاده می شود, اعتبار قرارداد یا قدرت اجرائی آن تنها به این دلیل که از داده پیام استفاده شده زایل نمی شود.

۴- دکتر جعفری لنگرودی- محمد جعفر: مبسوط ترمینولوژی حقوق. جلد اول تهران گنج دانش ۱۳۷۸.

۵- D. Van Gerven et P. Wery; Chronique de jurisprudence. Les obligations : Les sources ; 1985- 95 ; J.T. 1996 ; P.714 n73

برای بررسی دقیق مفاهیم ایجاب و قبول در حقوق اروپایی رجوع کنید به:

- J.L. AUBERT, Notions et rôles de l`offre et de l`acceptation dans la formation du contrat, paris, L.G.D.J. 1970(thèse)

۶- برای توضیح بیشتر رک بند (ب) ذیل الذکر . و برای ملاحظه شرائط ایجاب و قبول در اینترنت از دیدگاه حقوق بلژیک رک.

- E. MONTERO, « Internet et le droit des obligations conventionnelles », in Internet sous le regard du droit, Bruxelles, Ed. Du Jeune Barreau, 1997, n 9.

مخاطب شخص یا اشخاص معینی باشند پیشنهاد را ایجاب می‌دانند ولی هنگامی که پیشنهاد عموم مردم و اشخاص نامعین را مخاطب قرار داده باشد، در اینکه موضوع آن ایجاب است یا دعوت به ایجاب پاسخ واحدی وجود ندارد.

حقوق مقایسه‌ای:

در حقوق برخی کشورها مانند بلژیک بین ایجاب و دعوت به ایجاب تفاوتی قائل نشده‌اند. و عرضه کالا در ویترین فروشگاه‌ها، نمایشگاه‌ها، دستگاه های توزیع اتوماتیک کالا،، و حراجی‌های عمومی یا فهرست کالاهایی که مشخصات آنها بر روی شبکه اینترنت عرضه شده به منزله ایجاب تلقی می‌شود.[۷] و به محض موثر شدن قبولی صادره از سوی مشتری، عقد واقع می‌شود و فروشنده ملزم به تحویل کالا مطابق شرائط اعلامی می‌باشد. در فرض فوق‌الذکر باید توجه داشت که بر روی سایت‌های اینترنتی لیست و مشخصات کالاها عرضه شده و کالاهای مختلف تبلیغ گردیده است. با توجه به فناوری موجود می‌توانیم بر روی صفحات وب با هر فشاری که روی ماوس می‌دهیم از صفحه‌ای به صفحه دیگر برویم. وقتی که برای باز شدن صفحه معرفی کالا و مشخصات کالاها، روی ماوس فشار می‌دهیم و صفحه مربوطه باز می‌شود، این عمل قبولی تلقی نمی‌شود. اما وقتی که صفحه مربوط به تکمیل فرم سفارش کالا را باز می‌کنیم در شرائطی قرار می‌گیریم که تایید ما ممکن است قبولی تلقی شود و منجر به انعقاد قرارداد گردد. خصوصا" در موردی که همزمان با تکمیل و تایید فرم سفارش کالا بر روی شبکه، بهاء کالا نیز از طریق کارت‌های اعتباری و امثال آن پرداخت می‌گردد وقوع قرارداد بدیهی به نظر می رسد.

بـــر خـــلاف مراتب فوق، در حقوق انگلستان و آلمان به دقت بین ایجاب و دعوت به ایجاب (invitation ad offerendum) تفاوت قائل شده‌اند.[۸] در این کشورها هر اعلامی، ولو اینکه مشتمل برتمام شرائط اساسی برای انعقاد قرارداد باشد، ممکن است ایجاب تلقی نشود. فهرست کالاها و قیمت آنها که توسط پست برای اشخاص ارسال می‌شود و همچنین عرضه کالا در صفحات وب و گالری‌های مجازی یا در ویترین فروشگاه‌ها و سوپر مارکت‌های واقعی فقط دعوت به ایجاب تلقی می‌شود[۹]. در چنین شرائطی فرض بر این است که ابتدا مشتری برای خرید کالای داخل ویترین ایجاب خود را عرضه می‌نماید و فروشنده می‌تواند آنرا قبول یا رد کند. بنابراین مشتری که در یک سوپر مارکت کالا را انتخاب نموده است و برای پرداخت وجه آن به صندوق مراجعه می‌کند. فروشنده آزاد است که این ایجاب را قبول نموده پول را دریافت و یا آنرا رد کند. در این سیستم فروشنده همیشه این شانس را دارد که در صورت کاهش شدید موجودی انبار یا تغییر قیمت‌ها، یا احتمال عدم ملائت مشتری و امثال آن با رد ایجاب از فروش و تحویل کالایی که برای فروش عرضه کرده بوده است خودداری نماید.

بند ۲ ماده ۱۴ کنوانسیون بیع بین‌المللی کالا (مصوب ۱۱ آوریل ۱۹۸۰ وین) از مفهوم ایجاب در حقوق انگلیس و آلمان تبعیت نموده و مقرر داشته است "پیشنهادی که مخاطب وی اشخاص معینی نیست صرفاً دعوت برای ایجاب محسوب می‌شود. مگر آنکه پیشنهاد کننده به وضوح خلاف آنرا تصریح نموده باشد". همانطور که ملاحظه می‌شود سیستم انگلیس و آلمان و همینطور کنوانسیون وین بین ایجاب به اشخاص معین و ایجاب به عموم تفاوت قائل شده و ایجاب به عموم را دعوت به ایجاب دانسته و

---

[7] - Marie De moulin la passation d`une commande sur les réseaux. In, Le commerce électronique européen sur les rails? Bruylant, Bruxelles, 2001, P.246 (sous la direction du prof. Etienne Montero)
8-P.D.V. MARAH, Comparative contract law: England, France, Germany, Aldershot. Gower, 1994, PP.42 ET s,: C. Witz, Droit privé allemande, vol. I, paris, Litec, 1992, PP. 133 et s.

۹- مع‌الوصف در حقوق آلمان این مسئله بین نویسندگان مورد اختلاف است. به عنوان مثال رک:

C. Witz, Droit privé allemand, op.cit.p.134

معتقد هستند که در این حالت فروشنده به عموم پیشنهاد نموده است که در صورت تمایل برای خرید کالا، ایجاب خود را به وی اعلام نمایند تا پس از قبول فروشنده عقد واقع شود.

در مورد وضعیت و مفهوم ایجاب در قراردادهای منعقده از طریق واسطه‌های الکترونیک، قانون نمونه آنسیترال و به تبع آن قوانین تجارت الکترونیک کشورها، من جمله قانون ایران حکم خاصی ارائه ننموده و این قبیل امور را به قواعد عمومی ارجاع داده اند. لذا می‌توان گفت که در هر مورد باید دید قانون حاکم بر قرارداد چه سیستمی را قبول کرده است. و باید مشخص نمود مطابق قانون حاکم بر قرارداد این عمل ایجاب محسوب می‌شود یا دعوت به ایجاب؟ البته در مورد کشورهای عضو کنوانسیون وین می‌توان همین کنوانسیون را اعمال نمود. و گفت در مورد عملیات انجام شده از طریق واسطه‌های الکترونیک نیز فقط پیشنهاد به اشخاص معین ایجاب تلقی می‌شوند. و پیشنهاد به عموم و اشخاص نامعین صرفا" به مفهوم دعوت به ایجاب می‌باشند.

مع الوصف باید توجه داشت که اولا" قواعد کنوانسیون وین آمره نیستند و طرفین می‌توانند بر خلاف آن تراضی نمایند. ثانیا" قلمرو حاکمیت این کنوانسیون از نظر موضوعی و مکانی محدود است. مثلا" شامل خرید و فروش سهام و اوراق بهادار، بیع کشتی ها، هواپیماها، هاور کرافت‌ها و همچنین شامل نیروی برق و کالاهایی که برای مصارف شخصی و خانوادگی خریداری می‌شوند و شامل خرید و فروش خدمات نمی‌گردد[۱۰]. بعلاوه، همانطور که ملاحظه شد این کنوانسیون فقط در رابطه بین تجار حکومت می‌کند و در مورد مصرف‌کنندگان حاکم نیست[۱۱].

به هر حال مطابق کنوانسیون وین، در مورد کالاهای عرضه شده بر روی صفحات وب که معمولا" مخاطب معین ندارند، ایجاب از سوی مشتریان اعلام می‌شود و قبولی از سوی فروشنده. لذا در این صورت وقتی که مشتریان از گالری‌های مجازی کالا را انتخاب و مطابق فرم‌های اعلام شده بر روی سایت‌های اینترنتی سفارش ارسال کالا را می‌دهند هنوز قراردادی منعقد نشده است. وقتی قرارداد منعقد می‌شود و طرفین ملزم به آثار آن می‌شوند که فروشنده به این سفارش پاسخ مثبت بدهد. مع الوصف از آنجا که در قراردادهای الکترونیکی، معمولا" مخاطب‌ها محدود نیستند و پیشنهاد به عموم اشخاص عرضه می‌شود، هیچ کنترلی بر روی اشخاصی که به صورت آن لاین وارد معامله می‌شوند وجود ندارد. و میزان دارایی و جدیت آنان جهت انجام معامله برای فروشنده معلوم نیست. ایجاب بی قید و شرط به عموم خالی از ریسک نیست. خصوصاً هنگامی که به ماهیت بین‌المللی شبکه‌ها توجه کنیم و بدانیم که در آن واحد ممکن است کسانی از ژاپن یا آفریقا یا آمریکا و... بر روی شبکه به پیشنهاد ما پاسخ بدهند، این خطر مضاعف می‌شود. زیرا همانطور که دیدیم ممکن است در مواردی پیشنهاد به عموم را نیز به معنی ایجاب الزام‌آور بدانند. لذا توصیه شده است که اگر قصد داریم معرفی و تبلیغ کالاهای ما بر روی سایت به معنای ایجاب تلقی نشود و با قبولی طرف مقابل ماخوذ به آثار قرارداد نشویم. لازم است به نحوی شایسته و قطعی موضوع را تعیین تکلیف نماییم. پیشنهاد می‌گردد عباراتی مانند "بدون الزام از طرف ما"، "هر قراردادی پس از تایید نهایی ما منعقد می‌شود" یا "سفارشات بالاتر از .... دلار که از سوی مشتریان ارائه می‌شود باید مورد قبول ما قرار بگیرد"[۱۲] و امثال آن در متن پیام منتشر

۱۱- رک مواد ۱ و ۲ کنوانسیون وین ۱۹۸۰ ناظر به بیع بین‌المللی کالا.

M. FALLON et D. Philippe, “La Convention de Vienne sur les contrats de vente internationale de marchandises”, J.T., 19998, P. 17.

۱۲- Mousseron, J.M: Technique contractuelle, ed. Lefebvre 2iem ed. 1999.

شده بر روی سایت گنجانده شود.[13] همچنین ممکن است یک ایجاب محدود به منطقه جغرافیایی خاصی مانند آسیا، ایران و امثال آن بشود. در این صورت پیشنهاد مزبور فقط نسبت به مخاطبینی که در این مناطق قرار دارند ایجاب محسوب می‌شود. این امر مانع از آن نیست که سایر اشخاص که در مناطق دیگر ساکن هستند آنرا نوعی دعوت به ایجاب تلقی نمایند و برای معامله با پیشنهاد دهنده اولیه به جای قبولی، ایجاب خود را به وی عرضه نمایند. در قرارداد نمونه‌ای که از سوی اطاق صنعت و تجارت پاریس برای تجارت الکترونیک تهیه شده از این مکانیزم استفاده شده است. از این مکانیزم تحت عنوان clause du territoire (شرط سرزمینی) یاد شده است.[۱۴]

مبحث دوم: انعقاد قرارداد از راه دور (contrat à distance):[۱۵]

هنگامی که طرفین قرارداد در یک جلسه حضور ندارند و از راه دور با یکدیگر ارتباط برقرار می‌کنند، معمولاً ایجاب و قبول به طور همزمان و مقارن انجام نمی‌شود و هر یک از ایجاب و قبول در مکان و زمان متفاوتی از سوی طرفین قرارداد صادر می‌شود. قراردادهای منعقده از طریق واسطه‌های الکترونیک غالباً مشمول چنین وضعیتی هستند. در این حالت مسئله مهمی که مورد توجه قرار می‌گیرد مسئله زمان و مکان وقوع عقد است. وقتی که فروشنده مقیم تهران با اعلام مشخصات قیمت کالا بر روی سایت اختصاصی خود، عملاً و صریحاً برای فروش کالا یا خدمات به مخاطبین خود ایجاب می‌نماید و مخاطبین وی که مقیم آسیا، اروپا، آمریکا یا هر قاره دیگری هستند قبولی می‌دهند. با توجه به تفاوت زمانی و مکانی اقدامات آن لاین طرفین قرارداد، باید زمان و مکان ارسال و دریافت داده پیام معلوم گردد و همچنین معلوم گردد که قرارداد در چه زمانی و در کدام کشور منعقد شده است در غیر اینصورت و عدم تعیین زمان و مکان انعقاد قرارداد ابهامات و مسائل حقوقی زیادی در روابط فی مابین طرفین لاینحل باقی می‌ماند. لذا این مبحث را در سه بخش به شرح زیر بررسی می‌نماییم:

الف) اهمیت تشخیص زمان و مکان وقوع قرارداد.

ب) تعیین زمان و مکان وقوع قرارداد.

ج) زمان و مکان ارسال و دریافت داده پیام.

۱۳- البته باید توجه داشت که اعمال این شیوه با قوانین ناظر به حمایت از مصرف کنندگان در تعارض نباشد. مثلا" گفته شده است که فروشنده حق ندارد هنگام امضای قرارداد از طرفی تعهد فوری و قطعی را بر عهده خریدار قرار دهد و از طرف دیگر شرائطی قید کند که به وی حق میدهند بطور یکجانبه قرارداد را کان لم یکن نماید.رک:

-Ch. Biquet Mathieu et J. Decharneux : Aspects de la conclusion du contrat par voie électronique. In- Le commerce électronique : Un nouveau mode de contracter ? A.S.B.L Edition du Jeune Barreau de Liège 2001. p. 154

۱۴- رک به:

Breese, p: Guide juridique de l`inrernet, vuibert, 2000 p. 188.

۱۵- این نوع قراردادها را عقد بین غائبین (Le contrat entre absents)نیزگفته‌اند. البته برخی نویسندگان قراردادهائی را که از طریق تلفن منعقد می‌شوند را عقد بین حاضرین (Le contrat entre parties présentes) دانسته‌اند. به عنوان نمونه رک:

J. GHESTIN , Le contrat : Formation, Traité de droit civil sous La direction de J. GHESTIN, t. II, 2iem éd., paris, L.G.D.J., 1988, n 243.

الف) اهمیت تشخیص زمان و مکان وقوع قرارداد:

اهمیت تشخیص زمان و مکان و قوع قرارداد از آثاری که بر آن مترتب است ناشی می‌شود. ذیلاً به برخی از این آثار به طور گذرا اشاره می‌نماییم.

۱- عدم امکان رجوع از ایجاب و قبول:

از لحظه وقوع عقد، هر یک از طرفین ملزم به اثر ایجاب یا قبول خود می‌گردد. حال آنکه قبل از لحظه وقوع قرارداد ممکن است ایجاب کننده بتواند از ایجاب خود رجوع نماید[۱۶] و همچنین قبول کننده ممکن است بتواند قبل از موثر شدن قبولی از آن منصرف گردد. بعد از لحظه وقوع قرارداد، دیگر ایجاب یا قبولی باقی نمانده تا از آن رجوع شود. از تلاقی ایجاب و قبول طرفین، فرزندی متولد می‌شود که قرارداد نام دارد. بنابراین تعیین زمان دقیق قرارداد بسیار مهم است.

۲- اهلیت طرفین قرارداد:

اشخاصی که دارای اهلیت برای اقدامات حقوقی و انعقاد قرارداد هستند ممکن است در زمانی محجور و فاقد اهلیت گردند. به عنوان مثال تاجری که دیروز در وضعیت بسیار مطلوب و خوبی به سر می‌برده ممکن است به هر دلیلی امروز مشاعر وی دچار اختلال شود یا گرفتار جنون گردد. همچنین تاجر ثروتمند و معتبر دیروز ممکن است به علت صدور حکم ورشکستگی وی امروز ورشکسته محسوب شود. همانطور که می‌دانید جنون از موارد حجر است و طبق ماده ۲۱۲ قانون مدنی معاملات محجور باطل است. ورشکسته نیز مطابق قانون تجارت از تصرف در اموال خود ممنوع است و معاملات وی حداقل غیر نافذ می‌باشد. در این حالت‌ها تعیین لحظه وقوع قرارداد بسیار حساس و حیاتی است. زیرا اگر در فرض‌های فوق‌الذکر، قرارداد قبل از جنون و ورشکستگی منعقد شده باشد صحیح و در غیر اینصورت باطل یا غیر نافذ می‌باشد.

۳- زمان انتقال مالکیت:

در بسیاری از سیستم‌های حقوقی مالکیت کالا همزمان با لحظه وقوع قرارداد از فروشنده به خریدار منتقل می‌شود. سیستم‌های حقوقی ناشی از کد ناپلئون و حقوق فرانسه قائل به انتقال اتوماتیک مالکیت همزمان با انعقاد قرارداد هستند. ماده ۱۵۸۳ قانون مدنی فرانسه در این زمینه مقرر می‌دارد که به محض توافق طرفین قرارداد در مورد کالا و بهاء آن قرارداد منعقد و مالکیت کالا به مشتری منتقل می‌گردد. هر چند که هنوز بهاء کالا پرداخت نشده و مبیع نیز تحویل نشده باشد. مطابق بند ۱ ماده ۳۶۲ قانون مدنی ایران نیز "به مجرد وقوع بیع مشتری مالک مبیع و بایع مالک ثمن می‌شود"[۱۷] بنابراین گاه زمان وقوع قرارداد مستقیماً تعیین کننده زمان انتقال مالکیت کالا به مشتری است.

۱۶- ایجاب ممکن است قابل رجوع (revocable) یا غیر قابل رجوع (irrevocable) باشد. فرض فوق ناظر به ایجاب قابل رجوع است. برای اطلاع بیشتر در این مورد و امکان انصراف از قبول رک. مواد ۱۶ و ۲۲ کنوانسیون وین ۱۹۸۰ (ناظر به بیع بین‌المللی کالا) و همچنین رک. دکتر داراب پور، مهراب: ترجمه کتاب تفسیری بر حقوق بیع بین‌المللی (کنوانسیون ۱۹۸۰ وین) جلد اول ۱۳۷۴ صفحه ۲۰۸ و بعد- همچنین صفحه ۲۶۳ و بعد.

۱۷- در حقوق برخی از کشورها وقوع عقد لزوماً و به طور اتوماتیک موجب انتقال مالکیت نمی‌شود. مثلاً طبق ماده ۹۳۳ قانون مدنی آلمان پس از وقوع عقد بیع فروشنده مکلف به تحویل کالا به مشتری و انتقال مالکیت آن به وی می‌باشد. چنانکه ملاحظه می‌شود فروشنده باید بعداً مالکیت را منتقل نماید: در کشورهای هلند، سوئیس، سوئد، یونان اسپانیا و برزیل نیز این مضمون **پذیرفته شده است. هر چند که** بند ب ماده ۴ کنوانسیون وین ۱۹۸۰ اثر قرارداد نسبت به انتقال مالکیت کالا را خارج از حیطه شمول مقررات کنوانسیون می‌داند اما از ذیل ماده ۳۰ این کنوانسیون که مقرر می‌دارد

٤- زمان شروع مرور زمان‌ها و مهلت‌ها:

معمولاً در قراردهایی که منعقد می‌گردد مبدأ زمان بندی مراحل پرداخت و تسلیم کالا از تاریخ وقوع قرارداد است. همچنین مطابق بند ج ماده ۳۳ کنوانسیون وین ۱۹۸۰ بایع مکلف است کالا را "ظرف مدت معقولی پس از انعقاد قرارداد" تحویل نماید. به علاوه ممکن است زمان وقوع عقد، لحظه شروع دوره گارانتی باشد.

٥- اصلاح و تغییر قوانین:

همزمان با اقدامات طرفین قرارداد برای انجام معامله و در فاصله بین ارسال و دریافت ایجاب و قبول، ممکن است قانونگذار ملی نیز مشغول اصلاح و بازنگری در برخی قوانین و مقررات مرتبط باشد. از آنجا که قراردادها قاعدتاً تابع قوانین زمان انعقاد خود هستند و اثر قوانین و مقررات ناظر به آینده است، لذا ممکن است مقرراتی که بعد از وقوع عقد تصویب می‌شوند عطف به ماسبق نشوند. از این جهت نیز لحظه وقوع عقد دارای اهمیت است. اگر زمان وقوع قرارداد معلوم نباشد در تعیین قانون حاکم بر قرارداد نیز مشکل خواهیم داشت. به علاوه اگر قرارداد در زمان حکومت قانون سابق منعقد شده باشد همان قانون بر وی حکومت می‌کند. و چنانچه پس از اصلاح قانون، قرارداد منعقد شده باشد قانون جدید بر آن حاکم خواهد بود. و این امر ممکن است از نظر شکلی و ماهوی حقوق طرفین قرارداد را دچار تحولات شگرف نماید.

هرچند که برخی از مسائل فوق‌الذکر (مانند مسئله اهلیت یا اصلاح و تغییر قوانین) که در انعقاد قرارداد از طریق پست و امثال آن مطرح می‌شود، در فرض انعقاد قراداد از طریق واسطه‌های الکترونیک، به دلیل آنکه سرعت عملیات بسیار زیاد است، کمتر صادق است. مع‌الوصف در موارد خاصی این مشکلات در قراردادهای الکترونیک نیز ظاهر می شوند. مثلاً در مورد فروش سهام شرکتها قیمتها سریع تغییر می نمایند و ممکن است از لحظه ارسال ایجاب تا لحظه وصول قبول تغییرات جدی در قیمت ایجاد شده باشد[۱۸]. بعلاوه به علت اشکالات فنی یا نقص دستگاه‌ها یا ترافیک شبکه‌ها گاه یک داده پیام الکترونیک نیز ممکن است پس از چند روز به مخاطب واصل شود.

مکان وقوع عقد نیز به نوبه خود مهم و مسئله ساز است. در بسیاری از نظام‌های حقوقی من جمله ایران تعهدات ناشی از عقود تابع قانون محل وقوع عقد است[۱۹] همچنین ممکن است صلاحیت سرزمینی دادگاه به محل ایجاد تعهدات مورد اختلاف (مکان وقوع عقد) بستگی داشته باشد[۲۰]. بنابراین تعیین مکان وقوع عقد نیز آثار حقوقی مهمی دارد. در قراردادهای الکترونیک با توجه به فناوری پیشرفته موجود، اصل ساز و مخاطب این امکان را دارند که در هر زمان و مکانی داده پیام را برای طرف مقابل ارسال و بدین وسیله به تبادل ایجاب و قبول بپردازند. ممکن است شخصی برای انعقاد قرارداد از محل کار اصلی یا فرعی خود یا از

بایع باید مالکیت کالا را به مشتری منتقل کند معلوم است که کنوانسیون از حقوق آلمان و کشورهای فوق‌الذکر تبعیت نموده و زمان وقوع قرارداد را با زمان انتقال مالکیت کالا مقارن نمی‌داند. همچنین رک: دکتر سماواتی، حشمت ا...: حقوق معاملات بین‌المللی، ۱۳۷۷ ققنوس، صفحه ۵۷ و بعد دکتر داراب پور مهراب: مرجع پیشین، جلد اول، صفحه ۸۷ و جلد دوم صفحه ۶۵ و بعد.

[18]- R. JULIA-BARCELO, E. MONTERO et A. SALAUN, “La proposition de directive européenne sur le commerce électronique: questions choisies”, in, Commerce électronique: Le temps des certitudes, Cahiers du CRID, n 17, Bruxelles, Bruylant, 2000, P.25.

۱۹- ماده ۹۶۸ قانون مدنی ایران.

۲۰-بند ۲ ماده ۶۲۴ و بند ۳ ماده ۶۳۵ قانون قضایی بلژیک.

مکان عمومی یا حتی در حال پرواز بر فراز آسمانها و در هنگام سفر ایجاب یا قبولی خود را برای مخاطب ارسال نماید. در چنین حالتی حتی اگر زمان ارسال پیام در سیستمها و دستگاههای مبدا و مقصد درج شده باشد. مکان ارسال و دریافت پیام ممکن است نامعلوم باشد. بنابراین باید ضوابط یا معیارهایی در نظر گرفته شود تا در صورت بروز مشکل و ابهام در خصوص زمان و مکان وقوع عقد، به کمک آن معیارها و ضوابط موضوع حل و فصل گردد.

برای نیل به مقصد ذیلاً ابتدا زمان و مکان وقوع عقد را به طور کلی بررسی می نماییم (ب) تا بتوانیم متعاقبا" به کمک آن و با توجه به زمان و مکان ارسال و دریافت داده پیام لحظه وقوع عقد و محل انعقاد قرارداد در قراردادهای منعقده از طریق واسطه‌های الکترونیک را تعیین نماییم. (ج)

ب) زمان و مکان وقوع عقد در قرارداد از راه دور(Le contrat à distance):

برخلاف قراردادهایی که هنگام انعقاد آنها طرفین عقد حضور دارند و مستقیما" با یکدیگر قرارداد مورد نظر خود را قطعی می‌نمایند (Le contrat entre parties présentes)، در مورد قراردادهای منعقد شده از راه دور یا بین غائبین، طرفین عقد در یک جلسه حضور ندارند و ممکن است هر یک در نقطه‌ای از جهان پهناور باشند. به علاوه برخلاف قراردادهای منعقده از طریق تلفن که هر چند طرفین در دو نقطه مختلف حضور دارند اما حداقل تقارن و توالی زمانی بین ایجاب و قبول آنها وجود دارد[۲۱] در قراردادهای بین غائبین نه تنها طرفین قرارداد در یک نقطه حضور ندارند بلکه از نظر تقارن یا توالی زمانی و فاصله زمانی بین لحظه ایجاب و لحظه قبول نیز موضوع قابل تامل است. زیرا پس از ارسال ایجاب از طریق پست، تلکس، فاکس یا حتی از طریق شبکه‌های الکترونیک مانند e-mail و internet ممکن است به هر دلیلی از قبیل قطع بودن ارتباطات، خرابی دستگاهها یا تعطیل بودن دفتر کار مخاطب یا خاموش بودن دستگاه‌های گیرنده در مقصد، شخص مخاطب در زمان نامعلوم دیگری از داده پیام (ایجاب) مطلع گردد و پس از اطلاع، در فرصت مناسبی که آن هم دقیقاً معلوم نیست مبادرت به ارسال پاسخ یا ارسال قبولی نماید. همچنین ممکن است مخاطب ایجاب یا قبول، داده پیام ارسال شده را در مکانی غیر از محل کار خود، مثلاً در مسافرت، هتل، داخل هواپیما یا در هر مکان نامعلوم دیگری بازیافت و ملاحظه نماید. بنابراین مسئله‌ای که باید روشن شود این است که عقد در چه زمانی و در کجا منعقد شده است.

برای حل این مسئله راه‌حلهای مختلفی در نظر گرفته شده است. متاسفانه نظامها و سیستم‌های حقوقی مختلف در این مورد راه حل یکسانی را انتخاب ننموده‌اند. برخی از کشورها به تئوری‌های "اعلام"[۲۲] و "ارسال"[۲۳] تاسی نموده‌اند. بر اساس تئوری اول از لحظه‌ای که مخاطب ایجاب (قبول کننده) اراده خود مبنی بر قبولی ایجاب را اظهار و اعلام می‌نماید عقد محقق می‌گردد. و بر اساس تئوری دوم از لحظه ارسال قبولی (خواه با پست یا سیستم‌های الکترونیک) قرارداد منعقد می‌گردد. این دو

۲۱- به همین دلیل قراردادهای تلفنی را قراردادهای حضوری دانسته‌اند و مشمول قراردادهای بین غائبین تلقی نکرده‌اند. رک:
J. GHESTIN, “Le contrat: formation, traite de droit civil sous la direction de J.GHESTIN, T.2, 2 ed. paris L.G.D.J. 1988 n243.

22- Théorie de la declaration.

23-théorie de l`expédition.

تئوری شباهت و قرابت بسیار زیادی دارند. بطوری که برخی آنها را تقریباً در یک مفهوم بکار برده‌اند.[۲۴] دراین تئوری‌ها اصلاً مهم نیست که ایجاب کننده از اعلام یا ارسال قبولی مطلع شده یا نشده باشد.[۲۵]

برخی دیگر از کشورها بیشتر به تئوری‌های وصول قبول[۲۶] و اطلاع از قبول[۲۷] توجه نموده‌اند.[۲۸] برای اینکه اراده طرفین قرارداد با یکدیگر تلاقی نموده و منجر به وقوع عقد شود. بر اساس تئوری وصول قبول، پیام قبولی باید به مخاطب وصول شده باشد. در این صورت فرض می‌شود که وی از مفاد قبولی مطلع است. طبق تئوری وصول قبول، چنانچه طرفین قرارداد در فضای الکترونیک عمل نمایند. قبولی ارسال شده از طریق واسطه‌های الکترونیک در زمان و مکان دریافت داده پیام بوسیله سیستم الکترونیک متعلق به مخاطب نافذ و قرارداد در همان لحظه منعقد می‌گردد.[۲۹] زیرا در این لحظه ایجاب کننده امکان مطلع شدن از قبولی را دارد. اما در تئوری اطلاع از قبول، برای وقوع عقد صرف وصول قبولی به مخاطب کافی نیست بلکه باید مخاطب از قبولی مطلع گردد. شایان ذکر است که در قراردادهایی که از طریق واسطه‌های الکترونیک مثلا" E-Mail منعقد می‌شود. ممکن است لحظه ارسال و دریافت پیام قبولی و نتیجتاً زمان وقوع عقد یکسان باشد. وقوع عقد از طریق واسطه‌های الکترونیک یکی از سئوالاتی که باید پاسخ داده شود. این است که اگر سیستم و دستگاه رایانه‌ای مخاطب که داده پیام به آن واصل شده مثلاً در شهر تهران مستقر باشد ولی مخاطب در هنگام سفر در شهر یا کشور دیگری داده پیام را از طریق دستگاه‌های رایانه‌ای که به آنها دسترسی پیدا می‌کند بازیافت نماید و از مفاد آن مطلع گردد، کدام مکان را باید مکان وقوع عقد دانست؟ برخی از نویسندگان معتقدند که این مسئله را باید با تکیه بر حاکمیت اراده طرفین قرارداد و با جستجو در شرائط قراردادی مقرر بین طرفین پاسخ گفت. مسلماً استفاده از مانورهای رایانه‌ای و حیله‌های ناشی از فناوری روز نباید منجر به این شود که حاکمیت اراده طرفین نادیده گرفته شود. بنابراین محل وقوع عقد مکانی است که با توجه به اوضاع و احوال و با توجه به مقررات ممکن است اراده طرفین عقد بر آن تعلق گرفته باشد[۳۰]. در هیچ حالتی نمی‌توان گفت، محلی که مخاطب به طور عملی و واقعی از داده پیام مربوط به قبولی مطلع شده محل وقوع عقد است. زیرا این امر به طور جدی مکان وقوع عقد را دستخوش تغییر و دگرگونی می‌کند و آنرا به خواست یکجانبه مخاطب قبولی (ایجاب کننده) موکول می‌نماید.[۳۱]

حقوق مقایسه‌ای:

24- Marie De moulin: “La passation d`une commande sur les réseaux” in. Le commerce électronique européen sur les rails ? OP.Cit. P. 248.

25-Marie De moulin: op. cit. P. 248, n 457

26-théorie de la réception.

27-théorie de l`information.

۲۸- در بسیاری موارد نتیجه این دو تئوری یکسان است. مانند قراردادهای منعقده با تلفن یا در قرارداد بین غائبین که پیام قبولی خواه از طریق الکترونیک یا وسایل سنتی همزمان با وصول به اطلاع مخاطب نیز می‌رسد.

۲۹- برا ی توضیحات بیشتر رک:

E.MONTERO, “Internet et le droit des obligations conventionnelles’ op. cit., n. 10, P.50.

30- E. Montero. همان منبع

۳۱- به هیمن دلیل در قانون نمونه آنسیترال و دستورالعمل‌های اتحادیه اروپا و قوانین تجارت الکترونیک اکثر کشورها برای مفهوم محل استقرار مؤسسه و بنگاه اقتصادی مکان تثبیت شده را ملاک قرار داده و به معیارهای فنی و متغیر ارجاع نداده‌اند. برای اطلاع بیشتر رک. مبحث زمان و مکان ارسال و وصول داده ذیل بند ج مبحث دوم همین مقالهTص ...و بعد

در حقوق فرانسه: از سال ۱۹۸۱ که دیوان کشور فرانسه در رابطه با قراردادهایی که از طریق پست منعقد شده‌اند مبادرت به صدور رأی نموده است.[۳۲] تئوری ارسال قبول پذیرفته شده و گفته‌اند زمان انعقاد قرارداد در چنین قراردادهایی مصادف با زمان ارسال نامه و تحویل آن به پست است و با رعایت تمام جوانب شاید بتوان همین راه حل را در مورد قراردادهای منعقده از طریق فاکس، تلکس یا قراردادهای منعقد شده از طریق واسطه‌های الکترونیک نیز اعمال نمود[۳۳].

نویسندگان حقوق مدنی ایران نیز نظریه ارسال قبول را برای تعیین تاریخ وقوع عقد پذیرفته‌اند. برخی گفته‌اند در عقدی که با مکاتبه انجام می‌شود و محل ایجاب و قبول متفاوت است عقد در محل قبول بسته می‌شود و زمان انعقاد آن تاریخ اعلام قطعی قبول (سپردن نامه حاوی آن به پست) است. مگر اینکه دو طرف به طور صریح یا ضمنی محل ایجاب و زمان وصول قبول به ایجاب کننده را محل و زمان وقوع عقد معین کرده باشند.[۳۴] همچنین استدلال شده است که، با توجه به ماده ۱۹۱ قانون مدنی که می‌گوید ((عقد محقق می‌شود به قصد انشاء به شرط مقرون بودن به چیزی که دلالت بر قصد کند.)) وصول قبول یا اطلاع از آن ضروری دانسته نشده است. بنابراین نظریه ارسال در حقوق ایران قابل دفاع می‌باشد.[۳۵]

در حقوق انگلستان نیز هنگامی که قبولی از طریق پست ارسال می‌شود قاعده معروف The Mail BOX Rule (قاعده صندوق پستی) حکومت می‌کند. و رویه قضایی انگلستان تئوری ارسال قبول را برگزیده و معتقد است که هنگام پست کردن نامه حاوی قبولی قرارداد منعقد می‌شود. قاعده صندوق پستی که در حقوق آمریکا نیز کاربرد دارد بسیار قدیمی است و ناشی از پرونده مشهور Adams v. lindsell (1818) می‌گردد.[۳۶] امروزه مشکلات ناشی از کندی و طولانی بودن ارتباطات حل شده و مدت زمان طولانی که بین لحظه ارسال قبولی تا لحظه وصول و اطلاع از قبولی وجود داشت به حداقل رسیده است. لذا باستثنای قاعده صندوق پستی در سایر موارد انگلیسیها نیز تئوری وصول قبول را پذیرفته‌اند.[۳۷] و این تئوری را در مورد قراردادهایی که از طریق تلفن، تلکس و به طریق اولی از طریق اینترنت منعقد می شود قابل اعمال می‌دانند. زیرا دراین موارد اگر داده پیام در ساعت کاری مخاطب به وی مخابره شود، و سیستم اطلاعاتی گیرنده قبولی در محل کار مخاطب نصب شده باشد تقریباً لحظه ارسال و وصول قبول به علت توالی سریع مقارن یکدیگر است.[۳۸] رویه قضایی انگلیس درمورد این مسئله هنگامی که قبولی در زمانی غیر از ساعات کاری مخاطب یا به محلی غیر از محیط کاری وی مخابره شده ساکت است.

در حقوق بلژیک تئوری وصول قبول را ملاک عمل قرار داده‌اند و ظاهراً منظور آنها این بوده که وصول به منزله اطلاع مفروض است، و اطلاع واقعی و بالفعل مخاطب را ضروری ندانسته‌اند. دکترین و رویه قضایی بلژیک متفقاً معتقدند که قرارداد در زمان و مکانی که ایجاب کننده از مفاد قبولی مطلع شده یا می‌توانسته مطلع شده باشد منعقد می‌گردد. و استدلال نموده‌اند

Cass. Fr., 7 janvier 1981, Bull. Civ., I, n 14, p. 11., Rev. trim. Dr. civ., 1981, p. 849, obs. CHABAS, Rev. trim. Dr. Com., 1981, p. 827, obs. J. HEMARD.

33-J. GHESTIN, Le contrat: formation Traité de droit civil sous La direction de J : GHESTIN, t . II, 2 éd., paris, L.G.D.J., 1988, P.281.

۳۴- دکتر کاتوزیان – ناصر (قواعد عمومی قراردادها) جلد ۱ شماره ۱۸۲ به بعد.

۳۵- دکتر شهیدی- مهدی تشکیل قراردادها و تعهدات, صفحه ۱۶۲.

36-Adams v. Lindsell (1818) 1 B & Ald 681, 106 ER 350, CA.

37-P.D.V. MARSH, Comparative contract law: England, France, Germany, aledershot, Gower, 1994, P.69.

38-Entores Ltd v. Miles Far East Corpn (1955) 2 QB 327, (1955) 2 ALL ER 493, Brinkibon Ltd v. Stahag Stahl und Stahlwarenhandel GmbH (1983) 2 AC 34, (1982) I ALL ER 293, HL.

که موکول نمودن نفوذ قبولی و انعقاد قرارداد به اطلاع واقعی مخاطب از مفاد قبولی از نظر اجرائی مشکلاتی ایجاد می‌کند. از آن جمله اینکه موجب می‌شود زمان وقوع عقد به احتمالات و یا اختیار شخص مخاطب موکول گردد.[39]

قانون مدنی آلمان نیز تئوری وصول قبولی را پذیرفته و در بند ۱ ماده ۱۳۰ مقرر داشته است که قبولی در لحظه وصول به مخاطب موثر و نافذ می‌گردد، مشروط بر اینکه انصراف از قبولی قبل یا همزمان با وصول قبولی به مخاطب نرسیده باشد.[۴۰]

در پایان این قسمت شایان ذکر است که کنوانسیون وین ۱۹۸۰ ناظر به بیع بین‌المللی کالا نیز اصل را بر پذیرش نظریه وصول قبول قرار داده است. و در کنار آن به نظریه ارسال قبول نیز توجه داشته است. این کنوانسیون در بند ۲ ماده ۱۸ مقرر داشته است: "قبول ایجاب از لحظه‌ای که اعلام رضا به ایجاب کننده واصل می‌گردد نافذ می‌شود..." وبرای روشنتر شدن مطلب در ماده ۲۳ تاکید نموده است که: ((قرارداد از لحظه ای که قبول ایجاب مطابق مقررات این کنوانسیون نافذ می‌شود، منعقد می‌گردد.)) چنانچه ملاحظه می‌شود کنوانسیون وین صریحاً زمان وصول قبولی را زمان وقوع عقد تلقی نموده است.[۴۱] البته با توجه به واقعیات و اوضاع و احوال حاکم بر روابط تجار، بند ۳ ماده ۱۸ این کنوانسیون به حاکمیت اراده طرفین نیز توجه نموده و تئوری ارسال قبول را نیز از نظر دور نداشته و مقرر نموده است که: ((معهذا چنانچه به موجب ایجاب یا در نتیجه رویه معمول به طرفین یا حسب عرف و عادت، مخاطب بدون اعلام به ایجاب کننده، بتواند با انجام عملی نظیر آنچه مربوط به ارسال کالا یا پرداخت ثمن است اعلام رضا نماید، قبول از لحظه‌ای که عمل انجام می‌شود نافذ است، مشروط بر اینکه عمل مزبور ظرف مدت مقرر در بند پیشین انجام شود.)) بنابراین مطابق کنوانسیون وین و همچنین حقوق آلمان، بلژیک و در مواردی حقوق انگلستان و... می‌توان گفت که در قراردادهای منعقده از طریق واسطه‌های الکترونیک اصولاً همزمان با اینکه داده پیام مربوط به قبولی به سیستم رایانه‌ای ایجاب کننده وارد گردیده و در دسترس وی قرار می‌گیرد عقد واقع می‌شود. مگر اینکه طرفین به گونه دیگری مقرر نموده باشند و به موجب این توافق بجای قبول لفظی، طرف قرارداد عملاً کالا را ارسال و ثمن معامله را به هر طریق ممکن مثلاً از طریق بانک یا کارت اعتباری بپردازد یا حواله نماید. در این صورت قرارداد از لحظه ارسال کالا یا پرداخت ثمن معامله منعقد می‌گردد. قانون نمونه آنسیترال و همچنین قانون تجارت الکترونیک ایران در مورد زمان وقوع عقد سکوت اختیار نموده‌اند. زیرا این مقررات به امور ماهوی توجه ندارد. اما در مورد زمان و مکان ارسال و دریافت داده پیام موضوع را به خوبی تعیین تکلیف نموده‌اند. لذا برای اینکه طبق قانون نمونه آنسیترال و قانون تجارت الکترونیک ایران زمان و مکان وقوع عقد را تعیین نماییم باید از سویی به تئوری‌های چهارگانه پیش‌گفته و موقعیت آنها در خقوق ماهوی کشورهای مختلف توجه نماییم و از سوی دیگر زمان و مکان ارسال و دریافت داده پیام از دید قوانین ناظر به تجارت الکترونیک را بررسی نماییم. بر اساس مطالب پیش گفته معلوم شد که برخی کشورها لحظه وصول قبول و برخی دیگر لحظه ارسال آنرا برای تعیین زمان عقد اساسی می دانند. اینک باید بدانیم در قراردادهای الکترونیک مقررات فوق‌الذکر چه زمانی را لحظه ارسال قبول و چه زمانی را لحظه وصول قبول تلقی می‌نمایند.

39-J. HEENEN, “L’acceptation de l’offre faite par correspondance » op. cit., n &-, p. 309.

۴۰- صدر این ماده مطابق صدر بند ۲ ماده ۱۸ و ذیل این ماده دقیقا" منطبق است با ماده ۲۲ کنوانسیون وین ۱۹۸۰ ناظر به بیع بین‌المللی کالا.

۴۱- مطابق ماده ۱۵ کنوانسیون وین ایجاب نیز از زمان وصول به مخاطب نافذ می‌گردد.

ج) زمان و مکان ارسال و وصول داده پیام:

همانطور که مشروحاً بیان شد بر اساس تئوری ارسال از لحظه‌ای که قبولی ارسال می‌گردد عقد واقع می‌شود. اما بر اساس تئوری وصول از لحظه‌ای که قبولی به مخاطب واصل می‌شود عقد محقق می‌گردد. سئوال این است که در قراردادهای منعقده از طریق شبکه‌های الکترونیک لحظه ارسال و لحظه وصول داده پیام چه زمانی است؟ ماده ۱۵ قانون نمونه آنسیترال و مواد ۲۶ الی ۳۰ از قانون تجارت الکترونیک ایران به این سئوال پاسخ داده‌اند. ابتدا زمان ارسال و وصول داده پیام و سپس مکان ارسال و وصول آنرا بررسی می‌کنیم.

۱- زمان ارسال و وصول داده پیام:

مطابق ماده ۲۶ قانون تجارت الکترونیک ایران که از بند ۱ ماده ۱۵ قانون نمونه برداشت شده است: "ارسال داده پیام زمانی تحقق می‌یابد که به یک سیستم اطلاعاتی خارج از کنترل اصل ساز یا قائم مقام وی وارد شود." این سیستم اطلاعاتی ممکن است متعلق به یک واسطه، مثلاً دفاتر گواهی امضاء یا متعلق به شخص مخاطب باشد. همچنین ممکن است سیستم اطلاعاتی مزبور متعلق به شخص ثالثی باشد که مخاطب برای ارسال پاسخ قبلاً آنرا تعیین نموده و مثلاً در متن ایجاب خود به مخاطبین اعلام نموده که پاسخ خود را به آدرس E-Mail متعلق به شخص خاصی ارسال نمایند. همانطور که ملاحظه می‌شود برخلاف تصور ما و علی‌رغم آنچه در فضای واقعی رخ می‌دهد، در فضای مجازی و الکترونیک ملاک تعیین زمان ارسال داده پیام (اعم از ایجاب یا قبول) ورود آن به سیستم اطلاعاتی خارج از کنترل اصل ساز است نه عمل اصل ساز (ایجاب کننده یا قبول کننده) که به منظور ارسال داده پیام روی دکمه صفحه کلید یا ماوس فشار می‌دهد. بنابراین اگر اصل ساز در تاریخ امروز داده پیام خود را مخابره نماید. اما به هر دلیلی، اعم از ترافیک شبکه یا خرابی سیستم‌های اطلاعاتی واسطه یا مخاطب، داده پیام فردا به سیستم خارج از کنترل اصل ساز وارد شود، زمان ارسال داده پیام فردا خواهد بود نه امروز. بنابراین داده پیامی که ارسال شده به هر دلیلی اگر به سیستم اطلاعاتی مخاطب وارد نشود، ارسال شده محسوب نمی‌شود. در موردی که سیستم اطلاعاتی مخاطب اصلاً کار نمی‌کند یا بد کار می‌کند، نه قانون نمونه آنسیترال و نه قانون تجارت الکترونیک ایران تصریحی ندارند. در رهنمودی که آنسیترال برای قانون نمونه مانحن فیه منتشر کرده تصریح شده است که در این حالت نیز نمی‌توان گفت که عمل ارسال داده پیام انجام شده است.[۴۲] در رابطه با زمان وصول داده پیام، ماده ۲۷ قانون تجارت الکترونیک ایران که دارای دو بند الف و ب می‌باشد و متناظر بند ۲ ماده ۱۵ قانون نمونه آنسیترال است، برای تبیین زمان وصول داده پیام دو فرض را در نظر گرفته است:

فرض اول آنست که مخاطب سیستم اطلاعاتی معینی را برای دریافت داده پیام تعیین کرده باشد. در این صورت دو حالت متصور است. ممکن است اصل ساز پیام را به سیستم اطلاعاتی تعیین شده بفرستد. در این حالت وصول داده پیام زمانی محقق می‌شود که داده پیام به همان سیستم اطلاعاتی وارد شود، ولو اینکه مخاطب از آن مطلع نشده باشد. ممکن است اصل ساز داده پیام را به یکی دیگر از سیستم‌های اطلاعاتی مخاطب و غیر از سیستمی که منحصراً برای این کار معین شده بفرستد. در این

42-Guide pour l'incorporation dans le droit interne de La loi type de La C.N.U.D.C.I sur le commerce électronique (1996) , in WWW. Uncitral/ Org. French/ texts P.30 n 104.

حالت از لحظه‌ای که این داده پیام توسط مخاطب بازیافت شود واصل شده تلقی می‌گردد نه لحظه‌ای که به این سیستم وارد شده است.[۴۳]

فرض دوم آنست که مخاطب یک سیستم اطلاعاتی معینی را برای دریافت داده پیام معین نکرده باشد. در این صورت به محض اینکه داده پیام به هر یک از سیستم‌های اطلاعاتی مخاطب وارد شود واصل شده تلقی می‌شود.[۴۴] وقتی می‌توان گفت داده پیام به سیستم اطلاعاتی مخاطب وارد شده که مخاطب بتواند آن را مورد بررسی و مطالعه قرار دهد. یکی از نکات قابل توجه در مورد مادتین ۲۶ و ۲۷ مانحن فیه این است که مطابق این مواد در بسیاری از موارد لحظه ارسال داده پیام و لحظه وصول آن یکسان و مقارن است. زیرا مطابق ماده ۲۶[۴۵] ارسال داده پیام زمانی تحقق می‌یابد که به یک سیستم اطلاعاتی خارج از کنترل اصل ساز یا قائم مقام وی وارد شود. این سیستم اطلاعاتی ممکن است متعلق به مخاطب باشد. و مطابق ماده ۲۷ وصول داده پیام نیز زمانی محقق می‌شود که داده پیام به سیستم اطلاعاتی مخاطب واصل شود.[۴۶] البته در این مورد استثنائاتی وجود دارد. اگر داده پیام به سیستم اطلاعاتی غیر از سیستمی که منحصراً برای این کار معین شده وارد شود وصول داده پیام از لحظه بازیافت آن محقق می‌گردد.[۴۷] مطابق بند ۳ ماده ۱۵ قانون نمونه آنسیترال و ماده ۲۸ قانون تجارت الکترونیک ایران محل استقرار سیستم‌های اطلاعاتی مخاطب هیچ تاثیری بر زمان دریافت داده پیام ندارد.

چنانکه ملاحظه می‌شود در مقررات ناظر به تجارت الکترونیک، زمان ارسال داده پیام عملاً در لحظه وصول داده پیام ادغام گردیده است و در قانون نمونه و قانون ایران آنچه مهم است لحظه وصول داده پیام به سیستم اطلاعاتی مخاطب است. بنابراین باید گفت تعارضی که در حقوق تجارت سنتی فی مابین کشورهای مختلف وجود دارد. و برخی نظریه ارسال قبول و برخی نظریه وصول قبول را برای زمان وقوع عقد معتبر دانسته‌اند در تجارت الکترونیک منتفی شده است. زیرا هر چند که برخی کشورها لحظه ارسال قبولی را و برخی دیگر لحظه وصول قبولی را لحظه وقوع قرارداد می‌دانند اما از آنجا که در قواعد تجارت الکترونیک فوق‌الذکر مفهوم ارسال در مفهوم وصول داده پیام ادغام شده، لحظه وقوع قرارداد در هر دو گروه کشورها می‌تواند همان لحظه ورود قبولی به سیستم اطلاعاتی مخاطب باشد. (به شرط آنکه همه از قانون نمونه پیروی کرده باشند) مثلاً چنانکه قبلاً ذکر شد نویسندگان حقوق مدنی ایران معتقدند که مطابق ماده ۱۹۱ قانون مدنی، در حقوق ما نظریه ارسال قبولی معتبر است. یعنی به محض ارسال قبولی قرارداد منعقد می‌شود. از آنجا که مطابق ماده ۲۶ قانون تجارت الکترونیک ایران ارسال وقتی محقق می‌شود که داده پیام مربوط به قبولی به سیستم اطلاعاتی خارج از کنترل اصل ساز وارد شود. و این سیستم در اغلب موارد ممکن است متعلق به مخاطب باشد. پس بنابراین لحظه وقوع قرارداد، زمانی است که قبولی به مخاطب واصل شده است. این امر مانند آن است که نظریه وصول قبولی را پذیرفته باشیم.

۴۳- بند الف ماده ۲۷ قانون تجارت الکترونیک ایران و بند a از پاراگراف ۲ ماده ۱۵ قانون نمونه آنسیترال.

۴۴- بند ب ماده ۲۷ قانون تجارت الکترونیک ایران و بند b از پاراگراف ۲ ماده ۱۵ قانون نمونه آنسیترال. همچنین ماده ۲۴ کنوانسیون بیع بین‌المللی کالا مصوب ۱۹۸۰ مقرر می‌دارد: "... ایجاب، اعلام قبول یا سایر انواع بیان اراده هنگامی به مخاطب واصل می‌شود که شفاها" به اطلاع وی رسانده شود، یا به طریق دیگر به شخص او، به محل تجارت یا به نشانی پستی‌اش و چنانچه محل تجارت یا نشانی پستی نداشته باشد به محل اقامت عادی او تحویل گردد.

۴۵- همچنین مطابق پاراگراف ۱ ماده ۱۵ قانون نمونه آنسیترال.

۴۶- رک پاراگراف ۱ بند الف ماده ۲۷ و بند ب ماده ۲۷ قانون مانحن فیه. همچنین رک بندهای a و b از پاراگراف ۲ ماده ۱۵ قانون نمونه آنسیترال.

۴۷- رک. پاراگراف ۲ از بند الف ماده ۲۷ قانون تجارت الکترونیک ایران و قسمت 2 از بند a از پاراگراف ۲ ماده ۱۵ قانون نمونه آنسیترال.

مسئله دیگری که مطرح می‌شود این است که چنانچه داده پیام به صورت غیر قابل فهم یا غیر قابل بهره‌برداری وارد سیستم اطلاعاتی مخاطب شود آیا واصل شده تلقی می‌گردد یا خیر؟ در این رابطه نیز قانون نمونه و قانون ما سکوت نموده‌اند. ماده ۳۰ قانون تجارت الکترونیک ایران آثار حقوقی زمان و مکان ارسال و دریافت داده پیام و محتوای داده پیام‌ها را تابع قواعد عمومی قرار داده است. اما این ماده چیزی از ابهام نمی‌کاهد. زیرا محل نزاع این است که آیا در صورت غیر قابل فهم بودن یا غیر قابل بهره‌برداری بودن داده پیام می‌توان آنرا دریافت شده تلقی نمود تاپس از آن در مورد محتوای آن و آثار حقوقی آن صحبت نماییم؟ لذا در مانحن فیه که معلوم نیست داده پیام دریافت شده تلقی می‌شود یا خیر، اصلاً نوبت به مفاد ماده ۳۰ نمی‌رسد. قانون نمونه آنسیترال نیز این امور را به قوانین ملی واگذار نموده و اساساً قصد آنرا ندارد که با ورود به چنین مباحثی با قوانین ملی در تعارض قرار گیرد. زیرا ممکن است در یک کشور صرف ورود پیام به سیستم اطلاعاتی بدون توجه به اینکه قابل فهم بوده یا نبوده باشد به منزله وصول پیام تلقی گردد. همچنین قانون نمونه به عرف معمول تجار نیز توجه دارد و نمی‌خواهد که برخلاف عرف‌های تجارتی مقرره‌ای وضع نماید.[۴۸] در عرف گاه ممکن است یک پیام رمز دار را قبل از رمز گشایی و قابل فهم شدن آن واصل شده تلقی نمایند. به علاوه مقررات ناظر به تجارت الکترونیک نباید شرائط مضیق تر و محدود کننده ای را به طرفین قرارداد تحمیل نمایند. وقتی که در فضای واقعی و تجارت سنتی، وصول پیام‌های رمزی و نامفهوم که بر روی اسناد کاغذی درج شده‌اند، گاه به منزله وصول پیام تلقی می‌شود، چرا پیام مشابه آن که به صورت داده پیام و از طریق واسطه‌های الکترونیک واصل می‌شوند مشمول چنین حکمی نباشند؟ مثلاً ممکن است اطلاعات و داده‌های رمزداری که ناظر به حقوق مالکیت فکری هستند و قابل فهم یا بهره‌برداری نیستند صرفاً جهت حفظ و نگهداری به مراجع ذیربط منتقل یا مخابره شوند.

در خاتمه شایان ذکر است که هرچند قانون تجارت الکترونیک در خصوص سئوالات فوق سکوت نموده، نمی‌توان واقعیات فوق‌الذکر را نادیده گرفت. از سوی دیگر باید توجه داشت که اگر ورود داده پیام‌های غیر قابل فهم به سیستم اطلاعاتی مخاطب به منزله وصول ایجاب یا قبول تلقی شود ممکن است زمینه سوء استفاده احتمالی اصل ساز را فراهم نماید. بنابراین تا زمان اصلاح و تکمیل قانون، برای پاسخ به این سئوال باید در هر مورد با توجه به موضوع و اوضاع و احوال خاص مربوطه تعیین تکلیف گردد.

۲- مکان ارسال و وصول داده پیام:

همانطور که قبلاً اشاره کردیم برخلاف تجارت سنتی که در آن با فضاها و اماکن ثابت و فیزیکی سر و کار داریم و معمولا" مکان ارسال نامه و محل دریافت آن معلوم است. شرایط و اوضاع و احوال حاکم بر فضای الکترونیک و توسعه روز افزون IT این امکان را فراهم نموده است که اشخاص بتوانند از هر نقطه جهان پیام خود را به نقطه دیگر ارسال نموده و در هر مکان مفروضی پیام واصله را دریافت نمایند. ممکن است شخصی از محل کار خود یا هنگام سفر در داخل هواپیما یا کشتی یا از هتلی در اقصا نقاط جهان به وسیله رایانه شخصی و قابل حمل یا رایانه‌های منصوب در هواپیماها و کشتی‌های مسافرتی یا سیستم‌های موجود در هتل‌ها و سایر اماکن عمومی داده پیام حاوی ایجاب یا قبول را ارسال یا دریافت نماید. لذا مکان واقعی ارسال و دریافت داده پیام به روشنی معلوم نیست. حال آنکه با توجه به مطالب پیش گفته مکان ارسال و دریافت داده پیام نقش

48- Uncitral: op. cit. n 103.

اساسی در تعیین آثار قرارداد ایفا می‌نماید. با وقوف به اهمیت این امر آنسیترال سعی نموده با اتخاذ معیارهایی از بروز مشکلات مربوط به آن پیشگیری نماید و قانونگذار ایران نیز از آن تبعیت نموده است.

۱- بند ۴ ماده ۱۵ قانون نمونه آنسیترال و ماده ۲۹ قانون تجارت الکترونیک ایران مسئله تعیین مکان ارسال و وصول داده پیام (ایجاب، قبول، یا هرگونه اعلام اراده دیگر) را به شرح ذیل حل و فصل نموده‌اند.

چنانچه طرفین قرارداد در خصوص مکان ارسال و وصول داده پیام به نحو خاصی توافق نموده باشند همین توافق ملاک عمل خواهد بود. در غیر اینصورت محل تجاری یا کاری اصل ساز (ارسال کننده) محل ارسال داده پیام است و محل تجاری یا کاری مخاطب محل دریافت آن تلقی می‌شود.

۲- اگر اصل ساز بیش از یک محل تجاری یا کاری داشته باشد، نزدیکترین محل به اصل معامله، محل تجاری یا کاری خواهد بود در غیر این صورت محل اصلی شرکت، محل تجاری یا کاری است.

۳- اگر اصل ساز یا مخاطب فاقد محل تجاری یا کاری باشند، اقامتگاه قانونی آنان ملاک خواهد بود.

ضمناً ماده ۳۰ قانون ایران آثار حقوقی زمان و مکان ارسال و دریافت داده پیام‌ها و همچنین آثار حقوقی ناشی از محتوای داده پیام‌ها را تابع قواعد عمومی قرار داده است.

نتیجه:

یکی از اهداف عمده استفاده از تجارت الکترونیک ایجاد سرعت و تسهیل انجام معاملات تجارتی است. یکی از اهداف Uncitral نیز این است که در جهت یکپارچگی قواعد تجارت بین‌الملل تمهیدات لازم را فراهم نموده و با پیشنهاد قواعد متحدالشکل روابط بین‌المللی تجار را تسهیل نماید. لذا قانون نمونه آنسیترال در مورد تجارت الکترونیک و به تبع آن قوانین مربوطه در کشورهای مختلف سعی نموده‌اند که حتی‌الامکان قواعد حقوقی حاکم بر تجارت الکترونیک با قواعد سنتی تجارت در کشورهای مختلف و همچنین با قواعد متحدالشکل تجارت بین‌المللی تفاوت نداشته باشد. تا استفاده از فضای الکترونیک در تجارت بین‌الملل کمترین اشکالات و تعارض‌های حقوقی را فراهم نماید.

چنانکه ملاحظه شد در مورد قواعد حاکم بر انعقاد قراردادها از طریق واسطه‌های الکترونیک نیز سعی شده است که فاصله‌ها و تفاوت‌های چشمگیر موجود فی مابین روش‌ها و ابزارهای تجارت سنتی و تجارت الکترونیک، کمترین تأثیر را بر جنبه‌های حقوقی موضوع تحمیل نماید. هر چند که قانون نمونه آنسیترال و قانون تجارت الکترونیک ایران در مورد مفهوم ایجاب و قبول حکم خاصی ارائه نداده‌اند. و اساساً قصد آنها نیز ورود به حیطه حقوق ماهوی نبوده و صریحاً اعتبار قراردادها و آثار عقود را تابع قواعد عمومی قرار داده‌اند. اما در تنظیم مقررات تجارت الکترونیک به خوبی سعی نموده‌اند که این مقررات حتی‌الامکان با قواعد عمومی مغایرت نداشته باشد.

در فضای واقعی وسنتی، نظام حقوقی اغلب کشورها در خصوص زمان وقوع عقد تئوری وصول قبول را پذیرفته‌اند. همچنین در کنوانسیون ۱۹۸۰ ناظر به بیع بین‌المللی کالا نیز اصل بر این است که ایجاب و قبول همزمان با وصول به مخاطب نافذ می‌شوند و زمان وصول قبول به مخاطب لحظه وقوع عقد می‌باشد. کنوانسیون فوق‌الذکر استثنائاً در صورتی که قبولی لفظی نباشد و مخاطب عملاً با ارسال کالا یا واریز وجه و پرداخت ثمن قبولی خود را اعلام کند تئوری ارسال را پذیرفته است. برخی از کشورها نیز تابع تئوری ارسال می‌باشند.

در فضای الکترونیک، مقررات قانون نمونه آنسیترال و قانون تجارت الکترونیک ایران در این خصوص به گونه‌ای تنظیم شده که نه تنها با قواعد فوق‌الذکر مغایرتی ندارد بلکه مکانیزم انتخاب شده در مقررات اخیرالذکر طوری طراحی شده که تعارض موجود بین طرفداران تئوری وصول و ارسال را نیز حل نموده است. همانطور که قبلاً بیان شده است از نظر این مقررات، داده پیام هنگامی ارسال شده تلقی می‌گردد که به سیستم اطلاعاتی خارج از کنترل اصل ساز یا قائم مقام وی وارد شود.[۴۹] ملاحظه می‌شود که در این صورت مفهوم ارسال در تجارت الکترونیک در اغلب موارد با مفهوم وصول منطبق است. زیرا معمولاً داده پیام وقتی به سیستم مخاطب یا قائم مقام او وارد شود (لحظه وصول عرفی) می‌توان گفت از کنترل اصل‌ساز خارج شده است. واین امر یعنی حذف عملی لحظه ارسال واقعی و ادغام مفهوم ارسال در لحظه وصول. از آنجا که قائلین به تئوری ارسال در فضای سنتی، برای درک مفهوم ارسال در فضای الکترونیک باید مطابق مقررات فوق عمل نموده و لحظه ورود داده پیام به سیستم اطلاعاتی مخاطب یا قائم مقام وی را لحظه ارسال تلقی کنند، عملاً در بسیاری از موارد لحظه ارسال و لحظه وصول قبول یکی خواهد شد. بنابراین خواه تئوری ارسال را پذیرفته باشیم و خواه معتقد به تئوری وصول قبول باشیم لحظه وقوع عقد یکسان خواهد بود واختلاف و تعارضی وجود نخواهد داشت.

در مورد مسئله شناور بودن مکان ارسال و دریافت داده پیام در فضای الکترونیک و اینکه اشخاص می‌توانند با استفاده از امکانات توسعه یافته و سیستم‌های رایانه‌ای در اماکن متعدد و نامعلومی مبادرت به ارسال یا دریافت پیام نمایند و این امر شبهه مضبوط نبودن مکان ارسال ودریافت داده پیام و در نتیجه نامعلوم شدن محل وقوع عقد را ایجاد می‌نماید. قانون نمونه آنسیترال و قانون تجارت الکترونیک ایران مسئله را به خوبی روشن نموده و امکان هرگونه تردید را از بین برده‌اند. این مقررات در غیاب توافق طرفین قرارداد، محل ارسال و دریافت داده پیام را تابع محل تجاری یا کاری طرفین یا اقامتگاه قانونی آنها قرار داده و اساساً محل استقرار سیستم اطلاعاتی طرفین را ملاک عمل قرار نداده‌اند.[۵۰] بنابراین در قراردادهای منعقده از طریق واسطه‌های الکترونیک مکان وقوع عقد نیز همواره محل تجارت یا کاری یا اقامتگاه قانونی مخاطب قبولی است، مگر آنکه خلاف آن توافق شده باشد.

۴۹- بند ۱ ماده ۱۵ قانون نمونه آنسیترال و ماده ۲۶ قانون تجارت الکترونیک ایران

۵۰- بندهای ۳ و ۴ ماده ۱۵ قانون نمونه و مادتین ۲۸ و ۲۹ قانون تجارت الکترونیک ایران.

☑ **عنوان: تاثیر اینترنت بر حق مؤلف در نظام حقوق بین‌الملل و حقوق کنونی ایران**

☑ **نویسنده: نوید رهبر** (دانشجوی کارشناسی ارشد حقوق خصوصی دانشگاه شهید بهشتی)

۱- مقدمه

با رشد روز افزون وسایل ارتباطات جمعی در دنیای کنونی و به خصوص اینترنت، بیش از پیش نظام حقوقی ما متحول گشته و تطبیق خود با این نوع فناوری‌ها ضروری به نظر می‌رسد. «اینترنت» در واقع مجموعه‌ای از شبکه‌ها می‌باشد که در ابتدا توسط بخش دفاعی ایالات متحده امریکا طراحی گردید[۱]، تا توسط آن در مقابل جنگ هسته‌ای و ارتباطات نظامیان مورد استفاده قرار گیرد. با عمومی شدن و استفاده همگانی از اینترنت بسیاری از فعالیت‌ها از جمله تبادل اطلاعات، کالا و خدمات از این طریق انجام می‌پذیرد.

بر اساس تحقیقات مؤسسه فارستر[۲] تجارت فرد به فرد[۳] از طریق اینترنت از ۴۸ میلیون دلار در سال ۱۹۹۸ میلادی به ۱,۵ تریلیون دلار در سال ۲۰۰۳ رسیده است. فروش کالاهای مصرفی از طریق اینترنت در حال رشد می‌باشد و این رشد از ۳,۹ بیلیون دلار در سال ۱۹۹۸ به ۱۰۸ بیلیون دلار در سال ۲۰۰۳ میلادی رسیده است.[۴] حدود ۱۰٪ از جمعیت دنیا آن‌لاین[۵] می‌باشند که حدوداً برابر با ۶۰۵ میلیون کاربر می‌باشد. پیش بینی می‌شود که این جمعیت در سال ۲۰۰۵ میلادی به یک بیلیون کاربر برسد[۶].

۱- http://www.netlingo.com/inframes.cfm

۲- Forrester Research Inc.

۳- Peer to Peer

۴- Street, F.Lawrence and Grant, Mark.P.(2002), Law of theInternet, US: Lexis Nexis,p 1.01

۵- قانون تجارت الکترونیکی برای واژه آن‌لاین(Online)، معادل برخطّ را گذاشته شده است که به دلیل آشنا بودن اذهان با عبارت آن‌لاین از واژه مذکور استفاده می‌شود. (ر.ک به ماده۶۶ قانون مزبور).م

۶- Seet Intellectual Property On The Internet: A survey Of Issues , p7, availableat http://ecommerce. Wipo.int/survey/index.html

ذکر این نکته ضروری است که با تصویب و ابلاغ قانون تجارت الکترونیک در روزنامه رسمی[۷]، حق مؤلف[۸] در نظام حقوقی ایران وارد مرحله تازه‌ای گردید. هرچند که تنها ۳ ماده به این مبحث مهم اختصاص یافته، با وجود این، وضع این مواد نیز از اهمیت فوق‌العاده‌ای برخوردار می‌باشد.

در این تحقیق بعد از بررسی اجمالی حق مؤلف در نظام حقوقی ایران و حقوق بین‌الملل، به تأثیر اینترنت و محیط دیجیتالی بر روی آن پرداخته و سپس به این مطلب می‌پردازیم که آیا نظام حقوقی ایران، پاسخگو به نیازهای ما در این زمینه می‌باشد یا خیر؟ و اینکه کنوانسیون‌های مهم بین‌المللی چه راه‌کارهایی را برای آن در نظر گرفته‌اند.

۲- حق مؤلف:

۲-۱- حقوق موضوعه ایران:

در این قسمت تنها به معرفی مختصر قوانین موجود در زمینه حقوق ادبی و هنری در ایران می‌پردازیم. در زمینه مزبور در ایران[۹] می‌توان به ترتیب تاریخی، به قوانین زیر مراجعه نمود:

- قانون حمایت حقوق مؤلفان، هنرمندان و مصنفان ۱۳۴۸
- قانون ترجمه و تکثیر کتب و نشریات و آثار صوتی ۱۳۵۲
- قانون حمایت از حقوق پدیدآورندگان نرم افزارهای رایانه‌ای ۱۳۷۹
- قانون تجارت الکترونیکی مصوب ۱۳۸۲

طبق ماده ۱ قانون حمایت حقوق مؤلفان، هنرمندان و مصنفان ۱۹۴۸ "به مؤلف و مصنف و هنرمند " پدید آورنده" و به آنچه از راه دانش یا هنر و یا ابتکار آنان پدید می‌آید بدون در نظر گرفتن طریق و یا روشی که در بیان و یا ظهور و یا ایجاد آن به کار رفته "اثر"اطلاق می‌شود." حقوق پدیدآورنده شامل حق انحصاری نشر، پخش، عرضه، اجرای اثر و حق بهره‌برداری مادی و معنوی از نام و اثر خود می‌باشد.[۱۰]

حق تکثیر و تجدید چاپ بهره‌برداری و نشر و پخش هر ترجمه‌ای با مترجم و یا وارث قانونی او بوده[۱۱] و در زمینه نرم‌افزارهای رایانه‌ای قانونگذار مقرر ساخته که "حق نشر، عرضه، اجرا و حق بهره‌برداری مادی و معنوی نرم‌افزارهای رایانه‌ای متعلق به پدید آورندگان آن است... ."

تحول اخیر حقوقی در زمینه حق مؤلف در بستر الکترونیکی و به خصوص اینترنت ماده ۶۲، ۶۳ و ۷۴ قانون تجارت الکترونیکی ایران می‌باشد. بر اساس ماده ۶۲ "حق تکثیر، اجرا و توزیع (عرضه و نشر) آثار تحت حمایت قانون حمایت حقوق مؤلفان، هنرمندان و مصنفان ۱۳۴۸/۹/۳ و قانون ترجمه و تکثیر کتب و نشریات و آثار صوتی ۱۳۵۲/۹/۲۶ و قانون حمایت از حقوق

۷- روزنامه رسمی شماره۱۷۱۶۷ مورخ شنبه ۱۱ بهمن ۱۳۸۲. این قانون ۱۵ روز بعد انتشار در روزنامه رسمی لازم الاجرا می‌رردد. م

۸- Copyright

۹- لایحه قانونی حمایت از حقوق ادبی و هنری زیر نظر دبیرخانه سازمان جهانی مالکیت معنوی (WIPO) تهیه شده است. م

۱۰- ماده ۳ قانون حمایت حقوق مؤلفان، هنرمندان و مصنفان ۱۳۴۸

۱۱- ماده ۱ قانون ترجمه و تکثیر کتب و نشریات و آثار صوتی ۱۳۵۲

پدیدآورندگان نرم‌افزارهای رایانه‌ای مصوب ۱۳۷۹/۱۰/۴، به صورت "داده پیام"[۱۲] منحصراً در اختیار مؤلف است. کلیه آثار و تألیفاتی که در قالب "داده پیام" می‌باشند، از جمله اطلاعات، نرم‌افزارها و برنامه‌های رایانه‌ای، ابزار و روش‌های رایانه‌ای و پایگاه‌های داده و همچنین حمایت از حقوق مالکیت فکری در بستر مبادلات الکترونیکی شامل حق اختراع، حق طراحی، حق مؤلف، حمایت از پایگاه داده، حمایت از نقشه مدارهای یکپارچه قطعات الکترونیکی و حمایت از اسرار تجاری مشمول قوانین مذکور در این ماده و قانون ثبت علائم اختراعات مصوب ۱۳۱۰/۴/۱ و آیین‌نامه اصلاحی اجرای قانون ثبت علائم تجاری و اختراعات مصوب ۱۳۳۷/۴/۱۴ خواهد بود، منوط بر آن که امور مذکور درآن دو قانون موافق مصوبات مجلس شورای اسلامی باشد.

تبصره ۲...

ماده ۶۳- اعمال موقت تکثیر، اجرا و توزیع اثر جزء لاینفک فراگرد فنی پردازش "داده پیام" در شبکه‌ها است از شمول مقرره فوق خارج است.

...

ماده ۷۴ در مورد ضمانت اجرای نقض حق مؤلف، اذعان می‌دارد: "هر کس در بستر مبادلات الکترونیکی با تکثیر، اجرا و توزیع (عرضه و نشر) مواردی که در قانون حمایت حقوق مؤلفان، هنرمندان و مصنفان ۱۳۴۸/۹/۳ و قانون ترجمه و تکثیر کتب و نشریات و آثار صوتی ۱۳۵۲/۹/۲۶ و قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای مصوب ۱۳۷۹/۱۰/۴، منوط بر آنکه امور مذکور طبق مصوبات مجلس شورای اسلامی مجاز شمرده شود، در صورتی که حق تصریح شده مؤلفان را نقض نماید به مجازات سه ماه تا یک سال حبس و جزای نقدی به میزان پنجاه میلیون ریال محکوم خواهد شد."[۱۳]

شروط حمایت یک اثر ادبی و هنری طبق قانون حمایت حقوق مؤلفان، هنرمندان و مصنفان و قانون ترجمه و تکثیر کتب و نشریات و آثار صوتی و قانونی حمایت از پدیدآورندگان نرم‌افزارهای رایانه‌ای به طور خلاصه از قرار ذیل می‌باشد:[۱۴]

الف) محسوس بودن شکل اثر[۱۵]

ب) اصیل بودن اثر[۱۶]

ج) چاپ و یا پخش یا نشر و یا اجرا یا توزیع برای نخستین بار در ایران[۱۷]

۱۲- "داده پیام (Data Message): هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی، نوری و یا فناوری‌های جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود." رک به بند الف ماده ۲ قانون تجارت الکترونیکی.م

۱۳- به نقد قانون تجارت الکترونیکی در زمینه حق مؤلف در بخش آخر پرداخته می‌شود

۱۴- توضیح و شرح هر کدام از خصایص زیر از حوصله این مقاله خارج است و به موارد مذکور تیتروار اشاره می‌گردد.م

۱۵- به معنی قابل دسترسی بودن، ملموس بودن و عینیت می‌باشد. م

۱۶- Original

۱۷- ماده ۲۲ قانون حمایت حقوق مؤلفان و مصنفان و هنرمندان مقرر می‌دارد: حقوق مادی پدیدآورنده موقعی از حمایت قانونی برخوردار خواهد بود که اثری **برای نخستین بار** در ایران چاپ و یا نشر و یا پخش نشده باشد. و ماده ۱۶ قانون حمایت از پدیدآورندگان نرم‌افزارهای رایانه‌ای اذعان می‌دارد:" حقوق مذکور در ماده ۱ [قانون حمایت از پدیدآورندگان نرم افزارهای رایانه ای] در صورتی مورد حمایت این قانون خواهد بود که موضوع برای نخستین بار در ایران تولید و توزیع شده باشد."

د) مالیات داشتن اثر

ه) اعلان مشخصات (منحصر به صفحات یا نوارهای موسیقی و صوتی)[۱۸]

*** ثبت اثر[۱۹]**

۲-۲- اسناد بین‌المللی

در سطح بین‌المللی مهمترین اسناد مربوط به آفرینشهای ادبی و علمی و هنری به قرار ذیل می‌باشند:

* Berne Convention 1886
* TRIPS Agreement 1994
* Universal Copyright 1952 (Revised 1971)
* WIPO Performance and Phonograms Treaty (WPPT)
* Rome Convention on Neighboring Rights 1961
* WIPO Copyright Treaty (WCT) 1996

در کنوانسیونهای TRIPS, Berne, Universal Copyright 1952 (Revised1971) و WCT که به حق مؤلف پرداخته‌اند، شرایطی را برای حمایت تعیین کرده‌اند. البته کنوانسیون TRIPS[20] و WCT[21] به کنوانسیون Berne می‌باشد. در همه این کنوانسیون ها، آثار ادبی، هنری و علمی در صورت داشتن خصایص "محسوب بودن" و "اصالت داشتن" از حمایت قانونی برخوردار خواهند بود.

۱۸- ماده ۴ قانون ترجمه و تکثیر کتب و نشریات و آثار صوتی حالت خاصی را که منحصر به صفحات یا نوارهای موسیقی و صوتی است به شرح زیر مقرر می‌دارد:
" صفحات یا نوارهای موسیقی و صوتی در صورتی حمایت می‌شود که در روی هر نسخه یا جلد آن علامت بین المللی پ لاتین (P) در داخل دایره و تاریخ انتشار و نام و نشانی تولید کننده و نماینده انحصاری و علام تجاری ذکر شده باشد."م

۱۹- ثبت اثر از شرایط شناسایی نیست و به عبارتی قانونگذار با عبارت *"می‌تواند"* این امر را مخیر کرده است. ماده ۲۲ قانون حمایت حقوق مؤلفان و مصنفان و هنرمندان اشعار می دارد:
"پدیدآورندگان می‌توانند اثر و نام و عنوان و نشانه ویژه اثر خود را در مراکزی که وزارت فرهنگ و هنر با تعیین نوع آثار آگهی می‌نماید به ثبت برساند. " هر چند اگر ثبت آن الزامی باشد اثبات آن در دادگاه و یا اماره مالکیت مفید به نظر می‌رسد. با توجه به مواد ۸ و ۹ قانون حمایت از پدیدآورندگان نرم‌افزارهای رایانه‌ای، ثبت نرم‌افزارهای موضوع مواد ۱ و ۲ قانون مزبور پس از صدور تاییدیه فنی توسط شورای عالی انفورماتیک حسب مورد توسط وزارت فرهنگ و ارشاد اسلامی و یا مرجع ثبت شرکت‌ها می‌باشد و دعوای نقض حقوق مورد حمایت این قانون، در صورتی در مراجع قضایی مسموع است که پیش از اقامه دعوی تاییدیه فنی شورای عالی انفورماتیک صادر شده باشد و الا دادگاه قرار عدم استماع دعوی صادر می‌نماید. البته قانونگذار استماع دعوی را منوط به تاییدسه شورای عالی انفورماتیک کرده است و به ثبت آن کاری ندارد. م

۲۰- نگاه کنید به مواد ۹ و ۱۰ کنوانسیون TRIPS.م

۲۱- نگاه کنید به مواد ۱ الی ۴ کنوانسیون WCT. م

کنوانسیون Berne پایه و اساس حمایت از "آثار ادبی و هنری"[۲۲] و مهمترین کنوانسیون بین‌المللی در حمایت از اینگونه آثار می‌باشد. آثار ادبی و هنری شامل هر گونه شکلی از خلاقیت در قالبهای زیر می‌باشد: هر نوع نوشته شامل: تخیلی و غیرتخیلی، علمی و متون فنی و برنامه‌های رایانه‌ای؛ پایگاه داده‌هایی که واجد خصیصه اصیل بودن به خاطر گردآوری و یا نظم و ترتیب و یا موضوع آن باشد[۲۳]؛ آثار موسیقی و صوتی و تصویری؛ آثار هنری شامل طراحی و نقاشی و عکاسی.[۲۴]
معاهدات WCT و WPPT[۲۵] که عموما به آنها "معاهدات اینترنتی" می‌گویند، وظیفه حمایت از حق مؤلف و مصنف و حقوق مرتبط و نیز روز آمد کردن کنوانسیون Berne با محیطهای مجازی و الکترونیکی را دارد.[۲۶]
مفاد معاهدات اینترنتی وایپو[۲۷] در گستره جهانی شبکه‌های مجازی که اینترنت را تشکیل می‌دهند بر سه قسمت عمده تقسیم می‌گردد.

- ❖ تکمیل بعضی جنبه‌های مربوط به موافقتنامه TRIPS که به صورت صریح و واضح در موافقتنامه مزبور، روشن نشده بود؛ مانند حمایت از برنامه‌های رایانه‌ای و یا پایگاه داده‌ها به عنوان آثار ادبی طبق قانون کپی رایت.
- ❖ به روزآمد کردن جنبه‌های مربوط به فناوری‌های دیجیتال (مانند دسترسی عموم در محیط دیجیتال).
- ❖ موادی که به طور خاص به تاثیر فناوری‌های دیجیتالی می‌پردازد.[28]

۳-۲- دکترین:

دکتر لنگرودی "حق معنوی" را اینطور تعریف کرده‌اند:
" حق معنوی یا (DRIOT INTELLLECTUEL) حقی است غیر از حق عینی و حق ذمی از این رو که نه به عین و نه به ذمه تعلق می‌گیرد بلکه مزیتی است قانونی و غیرمادی مانند حق مخترع بر اختراع خود و حقی که دارنده تصدیق رسمی

۲۲- این کنوانسیون از همه آثار ادبی و هنری (Literary and artistic work) حمایت می‌نماید.

۲۳- موضوع ماده ۱ قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای و ماده ۶۲ قانون تجارت الکترونیکی ایران.م

۲۴- در مورد حقوق مرتبط (Related Rights) در این مقاله بحث نمی‌شود اما به طور خلاصه حقوق مرتبط با حق مؤلف شامل حمایت از توزیع‌کنندگان و هر شخصی است که به ارزش آثار هنری و ادبی در ارائه به عموم، می‌افزاید؛ مانند خوانندگان و آهنگسازان، تولید کنندگان صفحات صوتی و ...

۲۵- معاهده WCT و WPPT به ترتیب در تاریخ ۶ مارس۲۰۰۲ میلادی و ۲۰ می ۲۰۰۲ میلادی لازم الاجرا گشته‌اند

۲۶- See "Intellectual Property On The Internet: A Survey Of Issues", p 31

۲۷- Winpo Internet Treaties

۲۸- 2bid,p32

دارد (از قبیل دیپلم، لیسانس و غیره) از این قبیل است حق مؤلف و حق کار فکری و حق صاحب اسم تجاری و حق سرقفلی و غیره... "[۲۹]

"الف) حق انحصاری استفاده از اختراع امور فکری مربوط به ادبیات، علوم، هنر، خواه به صورت کتبی، خواه به صورت گرافیک (تصویر– نقشه– خطوط) و تجسم و امثال آنها و نیز هر چیزی که با یک روش علمی تهیه می‌شود به شرط اینکه معرف شخصیت فکری تولید کننده باشد.

ب) حق مالکیت ناشی از حق انحصاری گفته شده در بالا را گویند.[۳۰]

مالکیت حق تألیف عبارت است از" اختیار قانونی نویسنده در مورد استفاده مالی از اثر قلمی خود در مدتی که قانون تعیین کرده است. "[۳۱]

دکتر فتحی درینی به نقل از ابوالحسن علی الحسنی الندوی حق تألیف را اینطور آورده است: "حق تألیف یعنی مؤلفی که پس از زحمتهای توان فرسای بسیار... توانسته کتابی ارزشمند پی نهد، حق دارد بهای زحماتش را دریافت کند یا ... عوض بگیرد."[۳۲]

با توجه به اینکه عنصر اصلی درحق تالیف ابداع و ابتکار است ضروری به نظر می‌رسد که در ماهیت آن نیز به مطالبی اشاره گردد.

به نظر دکتر نورالدین امامی" فعالیت اختراعی صور گوناگون دارد که در هر حال باید اصالت اختراعی داشته باشد... این فعالیت اعم است از اینکه به تنهایی بنیاد و اساس اختراعی را تشکیل دهد و یا صرفا" فکری باشد در زمینه یک اختراع یا طریقی برای تحقق یک اختراع و یا وسیله و تدبیری برای غلبه به مشکلات وصول به یک اختراع و یا تسهیل در نتیجه‌گیری از یک اختراع باشد."[۳۳] لذا در اختراع صرفاً ابداع یک چیز نو نیست پس هر گونه فکر و ارائه طریق برای وصول به یک نتیجه و یا رفع موانع یک اختراع اگر دارای خصیصه "اصالت" باشد یک اختراع و نوآوری است.

۲۹– ن.ک، لنگرودی جعفر (۱۳۷۶)، ترمینولوژی حقوق، انتشارات گنج دانش (تهران)، چاپ هشتم، ص ۲۲۷

۳۰– ن.ک همان منبع ص ۲۲۴

۳۱– ن.ک همان منبع ص ۶۰۰

۳۲– ن.ک درینی، فتحی (۱۳۷۶)، حقوق مؤلفان مترجمان و هنرمندان و ناشران در فقه معاصر، انتشارات هزاران (؟)، چاپ اول، ص ۹۷

۳۳– ن.ک امامی (۱۳۵۰)، حق مخترع (مطالعه تطبیقی فصلی از مالکیت فکری)، انتشارات دانشگاه تهران (تهران)، چاپ اول، ص ۵۵

۳- گذر حق مؤلف به محیط های دیجیتالی به خصوص اینترنت:

با توجه به افزایش تعداد کشورهایی[۳۴] که به اینترنت متصل شده‌اند و کاهش میزان قیمت دسترسی به اینترنت، این وسیله همگانی به طور مؤثری، محیط اطراف ما را تغییر داده است. شبکه اینترنت امروزه به عنوان وسیله‌ای برای تبادل اطلاعات، افکار و به تدریج کالا و خدمات مورد استفاده قرار می‌گیرد. اینترنت که با اهداف نظامی آغاز به کار کرد، پیش بینی می‌شود که در سال ۲۰۰۴ میلادی معاملات الکترونیکی معادل ۶ تریلیون دلار را پوشش دهد.[۳۵]

بسیاری ازشرکت ها در محیط اینترنت به خرید و فروش کالاها و خدماتی می‌پردازند که موضوع آنها مالکیت معنوی می‌باشد. برای مثال شرکت آمازون[۳۶] و یا بارنزاند نوبل[۳۷] و یا در ایران وب سایت http://www.iranbin.com به شما اجازه خرید کتاب، نوار موسیقی، فیلم و یا... را می‌دهد. همه این موضوعات در واقع نوعی از آثار تحت حمایت حقوق مالکیت معنوی می‌باشند که در اینترنت مورد خرید و فروش قرار می‌گیرند.

دیجیتالی شدن آثار مالکیت معنوی از طریق روندی که متن‌ها، تصاویر و صداها را به کدهای ۰ و ۱[۳۸] تبدیل می‌نماید و دسته‌بندی آنها در بیت‌ها و بایت‌ها، آنها را قادر می‌سازد تا از طریق شبکه اینترنت به تمام نقاط دنیا در کمترین زمان ممکن منتقل شوند. کتابهای الکترونیکی در قالب‌های Word و یا Pdf به راحتی از طریق گوشی‌های تلفن همراه و یا کامپیوترهای شخصی در تمام نقاط دنیا قابل دسترسی می‌باشند. با توجه به این خصیصه و سهولت دسترسی به اطلاعات از طریق اینترنت حقوق مالکیت معنوی و به خصوص حق مؤلف در وضعیتی جدید قرار می‌گیرد که عدم تهیه زیرساخت‌های مناسب و بستر قانونی می‌تواند مشکلات زیادی را در این راستا به وجود بیاورد.

مؤسسات و تولیدکنندگان آثار ادبی و هنری موضوع حقوق مالکیت معنوی به دنبال روش‌هایی برای در دسترس قراردادن آثار خود به صورت آن‌لاین می‌باشند. با توجه به خصیصه سهولت انتقال داده‌ها در محیط مجازی، امن‌سازی شبکه‌ها و استفاده از روش‌هایی قابل اطمینان و جلوگیری از سوء استفاده از آثار و نسخه‌برداری آن در محیط اینترنت یکی از مهمترین دغدغه‌های تولیدکنندگان این گونه آثار می‌باشد.[۳۹]

۳۴- تعداد کشورهایی که به اینترنت متصل شده اند در ده سال اخیر به طور فزاینده‌ای افزایش یافته است. در حالی که در ابتدای دهه ۱۹۹۰ نزدیک به ۱۰ کشور به اینترنت متصل بودند در سال ۲۰۰۱ این تعداد به ۲۱۴ کشور رسید. البته باید دانست که پراکندگی این دسترسی در نقاط مختلف دنیا بسیار مختلف بوده است. امریکایی شمالی با بیشترین میزان دسترسی، حداقل ۳۷٪ آسیا ۳۱٪ و اروپا ۲۹٪ را به خود اختصاص داده است. البته در ماه می سال ۲۰۰۲ میلادی کشورها و مناطقی که بیشترین میزان دسترسی به اینترنت را داشته‌اند، قاره اروپا بوده است. برای اطلاعات بیشتر رک به:
"Intellectual Property On The Internet: A Survey Of Issuess" , p8

۳۵- Ibid, p19

۳۶- www.amazon.com

۳۷- www.BarnsandNoble.com

۳۸- Binary codes

۳۹- یکی از مشکلات بزرگ کنونی در محیط مجازی اینترنت، سیستم فرد به فرد (Peer-to-Peer) می‌باشد. به کمک این سیستم، فایل‌های هر کاربر می‌تواند از طریق نرم‌افزار خاصی با دیگر کاربران به صورت مشترک استفاده گردد. فایل‌های موسیقی و فیلم و کتابهای الکترونیکی به راحتی از

مهمترین حق مؤلف، حق نسخه‌برداری و توزیع و نشر اثر خود در قالب‌های مختلف می‌باشد. این حق را هم در حقوق داخلی در ماده ۳ قانون حمایت حقوق مؤلفان و مصنفان و هنرمندان[۴۰] و نیز مواد [۴۱] و ۳[۴۲] قانون ترجمه و تکثیر کتب و نشریات آثار صوتی و ماده ۱ قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای[۴۳] و هم در کنوانسیون‌های بین‌المللی در بند ۱ ماده کنوانسیون Berne، ماده ۱۰ کنوانسیون رم، ماده ۱۴ موافقتنامه TRIPS و در مواد ۷ و ۱۱ معاهده WPPT اشاره شده است. این حق باید در تمامی نسخه‌برداری‌ها در محیطهای الکترونیکی اجرا می‌گردد. به این معنی که اثر موردنظر در حافظه رایانه یا سایر وسایل دیجیتالی نسخه‌برداری و ذخیره می‌گردد. این عمل در شبکه‌های مجازی چندین بار و در نقاط مختلف به وقوع می‌پیوندد. نسخه‌برداری مجدد در حافظه کوتاه مدت رایانه (RAM) به منظور انجام فعالیت‌های رایانه‌ای امری اجتناب‌ناپذیر است حال باید به این پرسش پاسخ داد که آیا هر دفعه نسخه‌برداری نیازمند اجازه مؤلف آن می‌باشد یا خیر؟ زیرا هر نسخه‌برداری نوعی نشر آن نیز محسوب می‌شود.

از دیگر مسائلی که باید در سطح بین‌المللی به آن پرداخت حدود حمایت از حق مؤلف در محیط دیجیتالی می‌باشد این حدود بایستی به صورت دقیق در سطح بین‌المللی تعریف گردد، زیرا نظام حمایت از حق مؤلف دوران بین دو مساله مهم می‌باشد؛

طریق این سیستم قابل دسترسی در رایانه‌های شخصی افراد می‌باشد از جمله برنامه‌های نرم‌افزاری که هم اکنون از نظام P2P حمایت می‌نمایند، برنامه KAAAZ می‌باشد که به راحتی از اینترنت قابل دریافت می‌باشد. م

۴۰- ماده۳- حقوق پدیدآورنده شامل حق انحصاری نشر و پخش و عرضه و اجرای اثر و حق بهره‌برداری مادی و معنوی از نام واثر اوست

۴۱- "ماده ۱- حق تکثیر یا تجدید چاپ و بهره برداری و نشر و پخش و عرضه و اجرای اثر و حق بهره‌برداری مادی و معنوی از نام و اثر اوست. "

۴۲-"ماده ۳- نسخه‌برداری یا ضبط یا تکثیر آثار صوتی که بر روی صفحه یا نوار یا هر وسیله دیگر ضبط شده است بدون اجازه صاحبان حق یا تولیدکنندگان انحصاری یا قائم مقام آنان برای فروش ممنوع است... "

۴۳- "ماده۱- حق نشر، عرضه، اجرا و حق بهره‌برداری مادی و معنوی نرم‌افزار رایانه‌ای متعلق به پدیدآورنده آن است... "

یعنی: حمایت از حقوق مؤلف و جلوگیری از انحصارگرایی. از طرفی نیز حمایت از منابع آزاد[۴۴] نرم‌افزاری مانند منابع ویندوزهای شرکت مایکروسافت و یا اجازه بهره‌برداری از آثار مؤلف و تعیین حدود مسئولیت‌ها و تعهدات به صورت قراردادی و قابلیت اجرای این قراردادها به پیچیده‌تر کردن قضایا اضافه می‌نماید.

همچنین مسئولیت فراهم آورندگان خدمات اینترنتی (ISP)[۴۵] در نقض حقوق مؤلف از دیگر دغدغه‌هایی است که باید در سطح بین‌المللی به آن توجه گردد. این که یک فراهم آورنده خدمات اینترنتی در صورتی که باعث نقض حقوق مؤلف گردد، برای مثال با فراهم آوردن فایل ها در وب سایت خود تسهیلاتی در دسترسی به آثار بدون اجازه مؤلف ایجاد نماید، چه مسئولیتی می‌تواند داشته باشد. و نیز بررسی نظام اشتراک فایل‌ها در محیط اینترنت به صورت فردفرد[۴۶] برای مثال فعالیت شرکت Napster و یا Kazza یکی از مباحث مهم و مبتلا به نظام حقوق مؤلف در سطح بین‌المللی می‌باشد.

با توجه به موارد مذکور در فوق و آشنایی با تأثیرات مهم محیط دیجیتالی بر روی حق مؤلف، بررسی وضعیت نظام حقوقی بین‌المللی و نظام حقوقی ایران به خصوص با تصویب قانون تجارت الکترونیک و راهکارهای آنها در مواجه با این مشکلات ضروری به نظر می‌رسد.

۱-۳- راهکارهای اسناد بین‌المللی:

درمورد اجازه نسخه‌برداری در محیط‌های الکترونیکی و دیجیتالی از آثار مؤلفین، ماده ۱۴ WPPT که در مورد حقوق مجریان[۴۷] است، اذعان می دارد: "تولیدکنندگان صفحات صوتی از طریق وسایل با سیم و بی‌سیم، از حق انحصاری اجازه در دسترس قرار دادن آثارشان به عموم بهره می‌برند، به نحوی که اعضاء جامعه به آن آثار، در هر زمانی و مکانی که اراده می‌نمایند. دسترسی داشته باشند." همین مضمون را ماده ۸ WPPT اعلام می‌دارد. نکته مهم در ماده مذکور این است که در این محیط برخلاف رسانه‌های جمعی مانند کانالهای تلویزیون و یا ماهواره، دریافت کننده قدرت انتخاب موضوع را دارد. به عبارتی دریافت کننده منفعل نیست.

آنچه از مواد بالا استنباط می‌گردد این است که در محیطهای الکترونیکی نیز نسخه‌برداری از آثار مورد حمایت حق مؤلف نیاز به اجازه مؤلف و تولید کننده اثر دارد.

همچنین ماده WCT11 و ماده WPPT۱۸ دول عضو را موظف می‌نماید تا حمایت های قانون کافی و شیوه‌های جبران خسارت مؤثر را در مقابل سوء استفاده از تدابیر فنی مؤثری که توسط مؤلف در رابطه با اعمال حقوق خود طبق این معاهده و

۴۴- Open sources

۴۵- Internet Service Providers and Internet content Providers (ISP&ICP)

۴۶- Peer-to-peer

۴۷- جزئی از «حقوق مرتبط» می‌باشد. م

کنوانسیون Berne به کار برده، فراهم آورند. در واقع امن ساختن شبکه‌ها و ایجاد ضمانت اجرا در صورت نقض حقوق مؤلف در محیطهای الکترونیکی جزء تبدابیر دولت‌های عضو می‌باشد.

از طرف دیگر دو معاهده WCT و WPPT روشی دیگر را برای حمایت از حقوق مؤلف در نظر گرفته‌اند. طبق ماده ۱۲ WCT و ماده ۱۹ WPPT دول عضو باید روش‌های جبران خسارت کافی و مؤثری را در مقابل هر کسی که با آگاهی[۴۸]، حقوقی که طبق کنوانسیون Berne به رسمیت شناخته شده، از طریق تحریک، فراهم آوردن، تسهیل یا پنهان کردن از طریق ارتکاب یکی از موارد زیر نقض کند، فراهم آورند:

- حذف یا تغییر هر گونه حقوق الکترونیکی اطلاعات مدیریتی[۴۹] بدون اجازه؛
- توزیع، واردات برای توزیع، پخش رادیویی و تلویزیونی و یا سایر صور انتقال آثار یا نسخه‌هایی از آن که به حذف یا تغییر حقوق اطلاعات مدیریتی آگاه باشد بدون اجازه به عموم.

حقوق اطلاعات مدیریتی،[۵۰] اطلاعاتی است که معرف اثر، مؤلف آن و مالک هر گونه حقوق مربوط به آن بوده و شامل هرگونه عدد یا کدی است که نشانگر چنین اطلاعاتی باشد، البته در زمانی که این اطلاعات به اثر الصاق شده و یا به نحوی در زمان ارائه به عموم نشان داده شود.[۵۱]

از این مواد نیز می‌توان مسئولیت فراهم آورندگان خدمات و محتویات اینترنتی (ICP&ISP) را استنباط نمود. هر چند به نحوه بررسی میزان مسئولیت اشاره‌ای نکرده است وآن را به دادگاه‌های داخلی کشورهای عضو واگذار کرده است.

تدابیر دولت‌ها علاوه بر موارد مذکور در فوق، شامل تولید فناوری‌هایی در مقابله با تکثیر آثار مانند وسایل غیرقابل نسخه‌برداری و کدگذاری، استفاده از رمز و غیره... می‌باشد. البته هنوز دولت‌ها به روشی بین‌المللی و متحدالشکل دست نیافته‌اند.

۲-۳- راه‌کارهای حقوق داخلی

تا قبل از تصویب قانون تجارت الکترونیکی، حمایت از حقوق مؤلف در محیط دیجیتالی در هاله‌ای از ابهام قرار داشت. تنها به حقوق مؤلف نرم‌افزارها در قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای توجه شده بود و به سایر حقوق مؤلف در محیط دیجیتالی اشاره‌ای نگردیده بود.

قانون تجارت الکترونیکی اولین قانونی است که در نظام حقوقی ایران به حمایت از حق مؤلف در محیط‌های الکترونیکی می‌پردازد[۵۲]. از طرفی نیز اولین بار است که به "حقوق مرتبط" پرداخته است.[۵۳]

۴۸- و یا با توجه به جبران خسارت مدنی، زمینه‌ای معقول برای آگاهی داشته باشد. ماده ۱۲

۴۹- Electroneic rights management infomation

۵۰- Rights management information

۵۱- ” Intellectua; Property On The Internet: A Survey Of Issues” ,p 35

همانطور که در بالا اشاره شده، خصیصه اصلی دیجیتالی شدن آثار حقوق مؤلف، نسخه‌برداری مجدد در محیط‌های دیجیتالی می‌باشد و بدون تردید این نسخه‌برداری به خصوص نسخه‌برداری در حافظه موقت نیازمند اجازه صاحب اثر می‌باشد. از طرفی طبق ماده ۲۲ قانون حمایت حقوق مؤلفان، هنرمندان و مصنفان ۱۹۴۸ در صورتی از یک اثر حمایت می‌گردد که آن اثر برای نخستین بار در ایران چاپ یا پخش یا نشر یا اجرا شده باشد و قبلاً در هیچ کشور دیگری چاپ یا نشر یا پخش یا اجرا نشده باشد و ماده ۱۶ قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای علاوه بر تولید در ایران شرط دیگری را برای حمایت از نرم‌افزار ایجاد می‌نماید و آن توزیع آن در ایران می‌باشد. استفاده از حرف عطف "واو" منجر به این برداشت می‌گردد. این ماه اذعان می دارد: "حقوق مذکور در ماده ۱ در صورتی مورد حمایت این قانون خواهد بود که موضوع برای نخستین بار در ایران تولید و توزیع شده باشد. " در کنار این مطلب با توجه به نسخه برداری‌های متعددی که در محیط دیجیتالی به وقوع می‌پیوندد اعم از نسخه‌برداری در حافظه موقت رایانه صاحب اثر و یا یارانه فراهم آورنده محتویات اینترنتی (ISP[54]) و یافراهم آورنده خدمات اینترنتی (ISP) عموماً اثر مورد نظر خارج از قلمرو ایران مورد نسخه‌برداری و توزیع قرار می‌گیرد و تعیین اینکه این توزیع یا نسخه‌برداری در ایران انجام شده است تقریبا امری محال می‌باشد. دیجیتالی شدن آثار و استفاده از شبکه‌های اینترنتی باعث توزیع آثار در اقصی نقاط دنیا می‌گردد و به عبارت دیگر دیجیتالی شدن مانع از شناسایی دقیق مبدأ توزیع یا نشر یا تولید و اجرا می‌باشد. فلذا حمایت از آثار فقط به قلمرو ایران محدود می‌گردد که این امر با خصیصه عدم محدودیت مرزی اطلاعات در محیط الکترونیکی و دیجیتالی در تعارض است و با توجه به اصل عدم، اثبات آن به عهده مدعی بوده که امری بسیار دشوار و یا محال می‌باشد.

از طرف دیگر توزیع و نشر آثار در محیط‌های مجازی و شبکه‌ای مانند اینترنت همانطور که در بالا ذکر شد متفاوت از مفهوم متداول توزیع و نشر می‌باشد. زیرا دریافت‌کنندگان در محیط‌های مجازی فعال بوده و مانند پخش از طریق تلویزیون و رادیو دریافت‌کنندگان "منفعل" نمی‌باشند. اینکه اثری در محیط مجازی برای عرضه به عموم منتشر گردد مفهومی متفاوت دارد که می بایست مورد توجه قانونگذار ما قرار می‌گرفت.

ایراد دیگری که به قانون تجارت الکترونیکی وارد است اضافه کردن قیدی برای حمایت است. طبق ماده ۷۴ "هرکس در بستر مبادلات الکترونیکی با تکثیر، اجرا و توزیع (عرضه و نشر) مواردی که در قانون حمایت حقوق مؤلفان، هنرمندان و مصنفان ۱۳۴۸/۹/۳ و قانون ترجمه و تکثیر کتب و نشریات و آثار صوتی ۱۳۵۲/۹/۲۶ و قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای مصوب ۱۳۷۹/۱۰/۴، منوط بر آنکه امور مذکور طبق مصوبات مجلس شورای اسلامی مجاز شمرده شود، در صورتی که حق تصریح شده مؤلفان را نقض نماید به مجازات سه ماه تا یک سال حبس و جزای نقدی به میزان پنجاه میلیون ریال محکوم خواهد شد. به عبارتی حقوق مورد حمایت در سه قانون مزبور را مقید به عبارت "منوط بر آنکه امور مذکور طبق مصوبات مجلس شورای اسلامی مجاز شمرده شود" کرده است، به این معنا که حقوق مندرج در قوانین مزبور در صورتی در بستر الکترونیکی از حمایت قانون برخوردار هستند که مجلس شورای اسلامی آنها را مجاز بشمارد و این بدیهی است که

۵۲- ماده ۶۲ قانون تجارت الکترونیکی.م

۵۳- برای توضیح مفهوم" حقوق مرتبط" به پاورقی شماره ۵ صفحه ۵ مراجعه نمایید.

۵۴- Internet Service Providers and Internet Content Providers (ISP&ICP)

خلاف اصاله الاباحه می‌باشد و مجلس شورای اسلامی در هر مورد باید تعیین نماید که کدام حق از حقوق مؤلف مجاز شناخته می‌شود یا نمی‌شود در صورتی که با تصویب سه قانون ۱۳۴۸،۱۳۵۲ و [۵۵]۱۳۷۹، مجاز بودن این حقوق را ابراز داشته است و اضافه کردن قید اشاره شده، باعث ایجاد این شبهه می‌باشد.

عدم توجه به انحصارگرایی[۵۶] در قانون تجارت الکترونیکی به خصوص صدور مجوزهای بهره‌برداری اجباری در صورتی که مؤلف از حق خود سوء استفاده نماید و یا استفاده‌ای غیر منصفانه به عمل آورد از ایرادات دیگر می‌باشد. عدم توجه به توازن انحصارگرایی و حمایت از حق مؤلف می‌تواند مشکلات زیادی را به دنبال داشته باشد که می‌توان برای مثال به از بین رفتن قدرت رقابت در بازار و ضعیف شدن اقتصاد کشور اشاره نمود.

از استعمال لفظ" هرکس" در ماده ۷۴ می توان به صورت غیرمستقیم مسئولیت فراهم آورندگان خدمات و محتویات اینترنتی را استنباط نمود. اما تعیین میزان دقیق این مسئولیت و تعیین حالات مختلف این مسئولیت و نیز تاثیر حقوق قراردادها و آزادی طرفین در تعیین میزان خسارات از اهمیت زیادی برخوردار است که قانون تجارت الکترونیکی به آن اشاره ننموده است.

اتخاذ سیاستی واضح نسبت به نظام اشتراک فایل‌ها به صورت فرد به فرد می‌توانست بستر مناسبی را برای توزیع و نشر آثار در محیط مجازی فراهم آورد. همچنین باعث ایجاد نظامی امن در بستر مبادلات الکترونیکی می‌گشت. در صورت واضح بودن این خط مشی و امن بودن محیط مجازی صاحب اثر به راحتی می‌توانست اثر خود را در محیط مجازی منتشر نماید. اما عدم تعیین این مسأله می‌تواند مانعی در راستای این مهم باشد.

از دیگر ایرادات قانون تجارت الکترونیکی در وضع مجازات، عدم تعیین قابل گذشت بودن و یا قبل گذشت نبودن جرائم مذکور می‌باشد و با توجه به این که ماده ۷۲۷ قانون مجازات اسلامی نیز قانون سابق بوده و اشاره‌ای نیز در قانون تجارت الکترونیکی به آن نشده به نظر می‌رسد که جرائم مذکور در قانون فوق، جرائمی غیرقابل گذشت می‌باشد اما نقض حقوق مؤلف دارای جنبه خصوصی بوده و غیرقابل گذشت انگاشتن آن، بی‌مورد است.

در آخر باید اشاره کرد که تصویب قانون تجارت الکترونیکی قدم مؤثری در ساخت بستری مناسب برای انجام فعالیت‌های تجاری و غیرتجاری در محیط الکترونیکی می‌باشد. اما در نظر گرفتن ماهیت بین‌المللی این قانون همانطور که صریحاً در بخش تفسیر در فصل سوم آن اشاره شده، از اهمیت غیرقابل انکاری برخوردار است. در بخش حقوق مؤلف قانون تجارت الکترونیکی، علی رغم تصریح خود قانون، به این جنبه توجه نگردیده است. ممکن است در مقابل استدلال شود که در نظر گرفتن این جنبه، باعث ورود خسارات زیادی به اقتصاد ایران خواهد شد، اما به هر حال، ما به سمتی پیش می‌رویم که مجبور به تطبیق خود با قواعد بین‌المللی می‌باشیم.

قانونی در یک نظام حقوقی موفق خواهد بود که با تمام دیگر اجزا نظام حقوقی سازگاری و تناسب داشته باشد و الا یا به قانونی متروک تبدیل شده و یا نه تنها از مشکلات نمی‌کاهد بلکه به آن اضافه می‌کند. به نظر می‌رسد، تصویب قانون تجارت الکترونیکی در زمینه حق مؤلف، تنها پوششی برای فرار از فشارهای بین‌المللی است و تنها به خصیصه سرزمینی بودن آن توجه

۵۵- حمایت حقوق مؤلفان، هنرمندان و منصفان ۱۳۴۸/۹/۳ و قانون ترجمه و تکثیر کتب و نشریات و آثار صوتی ۱۳۵۲/۹/۲۶ و قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای مصوب ۱۳۷۹/۱۰/۴

۵۶- Monopoly

شده و همانطور که گفته شد با خصیصه "دیجیتالی شدن" و گسترش اطلاعات در شبکه‌های اینترنتی در تعارض است. اما باید به نقاط قوت آن نیز توجه نمود که می‌توان به شناسایی حقوق مؤلف در زمینه‌های حقوق مرتبط با حق مؤلف، حمایت از پایگاه داده، حمایت از نقشه مدارهای یکپارچه قطعات الکترونیکی و حمایت از اسرار تجاری و غیره اشاره نمود.

☑ **عنوان: حقوق مادی و معنوی نرم افزارهای پدیدآمده در جریان استخدام**

☑ **نویسنده: دکتر علیرضا مسعودی**

(دکتری حقوق خصوصی از دانشگاه تهران - مدرس دانشگاه آزاد اسلامی واحد شمال تهران)

چکیده

نرم‌افزارها امروزه پیچیدگی خاصی پیدا کرده‌اند این پیچیدگی هم در خود نرم افزار و هم در فرآیند تولید آن مشهود است. بگونه‌ای که تهیه و تولید نرم افزار عموماً معلول تلاش دسته جمعی برخی افراد خبره و متخصص در این کار می‌باشد. این مهم عموماً در قالب شرکتهای نرم‌افزاری نمود پیدا می‌کند ولی تردیدی نیست که اشخاص حقیقی (بعنوان کارمند و مستخدم شخص حقوقی) هستند که کار تولید و توسعه نرم افزار را انجام می‌دهند. از لحاظ کلی و اصولی حقوق مادی و معنوی متعلق به خالق اثر است و مسئله مهمی که در خصوص قرارداد کار (اعم از کارگری و یا پیمانکاری) مطرح می‌شود این است که کپی رایت نرم‌افزارهایی که نتیجه این رابطه کاری است متعلق به چه کسی است.

کلید واژه‌ها

نرم افزار – حقوق مادی و معنوی – شخص حقوقی – استخدام

۱- رابطه کاری

رابطه کاری مورد بحث از نظر حقوقی میتواند در دو قالب و شکل کلی نمود پیدا کند:

۱- رابطه کارگری – کارفرمایی

۲- رابطه پیمانکاری – کارفرمایی

فرق و تفاوت عمده و اساسی بین این دو نوع از قراردادها در این است که اولاً موضوع قراردادهای پیمانکاری محصول و نتیجه کار است در حالیکه موضوع قرارداد کار، در اختیار قراردادن نیروی کار است ، ثانیاً اجرت مقاطعه کار بر حسب نتیجه کار و مزد کارگر بر حسب زمان انجام کار پرداخت می‌شود. ثالثاً پیمانکار استقلال اقتصادی دارد و برای انجام کار مورد تعهد خود کارکنانی را بکار می‌گیرد ولی کارگر شخصاً کار می‌کند و نمی‌تواند تعهدات خود را بوسیله دیگری انجام دهد. (۱)

دادگاههای انگلیس برای تعیین و تشخیص هریک از این دو دسته رابطه کاری، معیارهای مختلفی را بکار می‌برند اصلی‌ترین معیار در این زمینه معیار کنترل است و برای اعمال آن بایستی به سوالات زیر پاسخ داده شود: آیا کارفرما شرایط و ضوابطی که تحت آنها مستخدم بایستی کار کند را دیکته می‌کند یا خیر؟ آیا جنبه‌هایی از رابطه کاری همانند تعطیلات، پرداخت حقوق در

هنگام بیماری، حق بازنشستگی و مسئولیت پرداخت مالیات در مورد مستخدم وجود دارد یا خیر؟ اگر پاسخ به سوالات مثبت باشد، رابطه کارگری و اگر منفی باشد، رابطه پیمانکاری وجود دارد.

۲- حقوق مادی و معنوی

حقوق مادی در واقع به حق بهره‌برداری انحصاری اقتصادی از اثر (و در بحث ما، نرم افزار) بر می‌گردد و تنها مالک حقوق مادی است که می‌تواند حقوق خود ناشی از اثر را برای نشر، کپی، بهره برداری، اجرا و عرضه به عموم اعمال نموده و دیگران را از اعمال آن حقوق منع گرداند.

حقوق مادی بر طبق قواعد کلی محدود به مدت معینی بوده و پس از آن، استفاده و بهره برداری برای همگان آزاد و مجاز خواهد بود. از دیگر خصوصیات حقوق مادی آن است که قابل انتقال به غیر می‌باشد.(۲)

حقوق معنوی بر اساس مبانی فلسفی و ارتباطی است که بین شخصیت پدیدآورندهٔ اثر با آن وجود دارد.(۳) و مهمترین جنبه‌ها و آثار حقوق معنوی عبارتند از: یکی حق شناخته شدن بعنوان مولف و پدیدآورنده اثر، (حق انتساب) و دیگری حق مانع شدن دیگران از هرگونه تغییر و یا تحریف اثر (حق تمامیت اثر). (۴)

مهمترین ویژگی این گونه حقوق آن است که قابل انتقال به غیر نیستند(۵) و علی‌القاعده و بویژه در نظام حقوق مولف محدود به زمان و مکان نمی‌باشند.(۶)

لازم است خاطرنشان سازد که در ابتدا بین کامن لو (نظام مبتنی بر کپی رایت) و حقوق رومی- ژرمنی (نظام حقوق مولف) در این زمینه تفاوتهایی عمده و اساسی وجود داشت بگونه‌ای که حتی تا مدتها حقوق معنوی در نظام کامن لو پذیرفته نمی‌شد و این تفاوت در الفاظ استعمال شده نیز تجلی یافته است. حمایت از پدیدآورنده اثر در کامن لو، با تاکید بیشتر بر جنبه مادی اثر، کپی رایت (copyright)، خوانده می‌شود و در حقوق رومی–ژرمنی، بعنوان نشانه‌ای از اهمیت و توجه بیشتر به مولف و پدیدآورنده اثر، حق مولف(Droit d auteur) ، نامیده می‌شود.

مثلاً در انگلستان حقوق معنوی بطور کامل و همه جانبه بموجب قانون کپی رایت، طرحها و اختراعات مصوب ۱۹۸۸ پذیرفته شد. هر چند که قبل از آن نیز، قانون کپی رایت مصوب ۱۹۵۶ در بخش ۴۳ خود، حق اعتراض به انتساب غیر واقعی اثر را برای پدیدآورنده به رسمیت شناخته بود.(۷)

در ایالات متحده نیز قانون visual artists right مصوب ۱۹۹۰ حقوق معنوی را برای پدیدآورندگان اینگونه آثار پذیرفته است (۸) کنوانسیون برن ۱۹۷۱ در ماده ۶ مکرر خود، حقوق معنوی را پذیرفته است و ماده ۹ موافقتنامه جنبه‌های مالکیت معنوی سازمان تجارت جهانی– سند نهایی مذاکرات نهایی دور اروگوئه (trips) – در ماده ۹ خود مواد ۱ تا ۲۱ کنوانسیون برن را برای اعضاء لازم‌الاجرا شناخته با این قید که اعضاء حقوق یا تعهداتی در خصوص حقوق اعطایی بموجب ماده ۶ مکرر کنوانسیون یا حقوق ناشی از آن ندارند (۹) و ظاهراً این مسئله هم بخاطر پافشاری ایالات متحده بوده است. هیئت نمایندگی آمریکا در این خصوص نسبت به گنجاندن حقوق معنوی در موافقتنامه trips اعتراض نموده و اعلام کرده که ایالات متحده علاقه دارد تا حقوق معنوی از حداقل حمایتهای لازم محروم گردد. در عین حال ماده ۱۶ موافقتنامه که حقوق معنوی علائم تجاری شناخته شده را برسمیت شناخته مورد پذیرش ایالات متحده قرار گرفته است بنابراین تحت مقررات trips، مک دونالد نسبت به علامت تجاری خود حقوق معنوی دارد اما مهاتما گاندی نسبت به آثار خود چنین حقی ندارد.

(۱۰) از انجائیکه کل نظام حقوقی ما و قوانین و مقررات مصوب بیشتر متاثر از نظام رومی – ژرمنی می‌باشد، لذا در تمامی قوانین و مقرراتی که دراین زمینه تصویب گشته، حق معنوی پدید آورنده اثر لحاظ شده است، منجمله ماده ۴ قانون حمایت حق مولفان، منصفان و هنرمندان مصوب ۱۳۴۸. در خصوص حقوق نرم‌افزار نیز قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای مصوب ۱۳۷۹ در ماده یک خود، حقوق مادی و معنوی پدید آورنده نرم افزار را به رسمیت شناخته، النهایه مدت حقوق مادی را به ۳۰ سال محدود ساخته و مدت حقوق معنوی را نامحدود دانسته است.

۳– حقوق مادی اثر پدیدآمده در جریان استخدام

هدف از استخدام، انجام کاری توسط کارگر و یا پیمانکار برای کارفرماست و تردیدی نیست که منافع و عواید ناشی از کار انجام شده بایستی عاید کارفرما گردد، چراکه کارفرما ما به ازای مادی انجام کار توسط کارگر و یا پیمانکار را در قالب مزد و یا مبلغ پیمان به او پرداخته است. همانگونه که قبلاً نیز اشاره شد حقوق مادی پدیدآورنده قابل نقل و انتقال بوده و هرگونه قراردادی در این خصوص معتبر دانسته می‌شود.

بند ب ماده ۶ قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای در مقام تعیین وضعیت حقوق مادی نرم‌افزارهای پدیدآمده در جریان استخدام اشعار می‌دارد:

ب: اگر هدف از استخدام یا انعقاد قرارداد، پدیدآوردن نرم‌افزار مورد نظر بوده و یا پدیدآوردن آن، جزء موضوع قرارداد باشد، حقوق مادی مربوط و ... متعلق به استخدام کننده یا کارفرماست مگر اینکه در قرارداد به صورت دیگری پیش بینی شده باشد.

بند ۲ بخش۱۱ قانون ۱۹۸۸ انگلیس در مورد "کپی رایت، طرحها و اختراعات" نیز کپی رایت آثاری که در جریان استخدام ایجاد می‌شوند را متعلق به کارفرما می‌داند مگر اینکه توافق و قرارداد مخالف دیگری در میان باشد. در کشورهای کامن لو حتی گفته شده است که اگر اثری در منزل مستخدم ولی با همان ایده و ماهیت موضوع و هدف قرارداد پدید آید، متعلق به کارفرما خواهد بود. (۱۱) چنین ترتیبی منطقی و صحیح است زیرا همانگونه که گفته شد، کارفرما مابه ازای مادی کار انجام شده توسط کارگر و یا پیمانکار را پرداخت می‌نماید و هدف از استخدام نیز پدیدآوردن اثر است پس در واقع کارگر یا پیمانکار برای کارفرما کاری انجام داده (پدیدآوردن اثر) و در قبال آن مزد یا حق الزحمه دریافت نموده است و بدیهی است حقوق مادی متعلق به اثر حاصل از چنین رابطهای باید عاید کارفرما گردد. قانون ایران با قید عبارت ً ناشی از استخدام یا قرارداد ً در ماده ۶ قانون موصوف هیچ تردیدی در شمول آن نسبت به قراردادهای پیمانکاری باقی نگذاشته است. و اگر چنین تصریحی نمی‌شد، ممکن بود در این خصوص شک و شبهه‌ای حاصل شود زیرا اطلاق عنوان استخدام بر رابطه کارفرما– پیمانکار دور از ذهن و غیر متعارف است.

قانونگذار پس از بیان حکم کلی راجع به تعلق حقوق مادی به کارفرما یا استخدام کننده، در انتهای ماده شرط خلاف مقرره قانونی یادشده را نیز مجاز دانسته است. لذا طرفین می‌توانند بنحو دیگری توافق نموده و مثلاً حقوق مادی ناشی از نرم افزار پدیدآمده در جریان کار را بالمناصفه متعلق به مستخدم و کارفرما دانسته و یا آنکه آنرا کلاً متعلق به مستخدم بدانند. تردیدی نیست که چنین قراردادی نیز طبق ماده ۱۰ قانون مدنی معتبر و لازم الاجراست. منتهی بایستی توجه داشت همانگونه که خود قانون نیز صراحت دارد، هدف از استخدام یا انعقاد قرارداد باید پدیدآوردن نرم افزار باشد یا پدیدآمدن آن جزء موضوع

قرارداد باشد و الا اگر مستخدم در کنار فعالیتهای عادی و روزمره کاری خود مبادرت به تهیه و خلق نرم افـزاری جهـت انجـام بهتر امور محوله بنماید، در اینصورت موضوع مشمول حکم ماده ۶ قانون نمی‌شود بلکه علی القاعـده بایسـتی مالکیـت حقـوق مادی را متعلق به پدیدآورنده (مستخدم) دانست. البته در این میان مسائلی از قبیل اینکه آیا مستخدم از امکانات و منابع کارفرما برای تولید اثر استفاده نموده یا خیر و اینکه آیا اثر در طول ساعات اداری تولید شده یا نـه، مسـائل کلیـدی در تعیـین مالکیـت حقوق مادی نرم‌افزار هستند.

٤- حقوق معنوی اثر پدیدآمده در جریان استخدام

همانگونه که اشاره شد حقوق معنوی قابل نقل و انتقال نمی‌باشند و به تعبیری، آثار پدیدآمده همچون بخـش جاودانـه وجود پدیدآورنده است. (۱۲) تلقی این حق بعنوان یک رابطه فلسفی و معنوی و ممنوعیت نقل و انتقـال حقـوق معنـوی کـه در همه سیستمهای حقوقی پذیرفته شده، در واقع ناشی از ماهیت و طبع اینگونه حقوق است. اصلی‌ترین نوع حقوق معنوی قابلیت انتساب اثر به پدیدآورنده است و اگر قائل بدان باشیم که چنین حق قابل انتقال است، در واقعی بنوعی تحریف واقعیـت و قلـب حقیقت رخ خواهد داد چون با اینکار پدیدآورنده را شخصی معرفی می‌کنیم که در واقع پدیدآورنده و خالق اثر نبوده است.

مساله مهمی که در رابطه با خلق و تولید نرم افزار مطرح است اینکه باتوجه به طبع کار و بر خلاف دیگر آثار هنـری و ادبی مشمول کپی رایت، خلق نرم افزار معلول تلاش دسته جمعی گروهی است که به این منظور دورهم جمع شده‌اند لذا بیشتر نرم‌افزارها در شرکتها و موسساتی تولید می‌شود که بصورت سیستماتیک، منظم و برنامه‌ریزی شده و با تقسیم کـار مبـادرت بـه تولید نرم افزار می‌نمایند. در این میان این مساله قابل توجه و تعمق است که ایا شخص حقوقی می‌تواند مالـک حقـوق معنـوی نرم افزار تلقی شود یا خیر؟ برخی در این زمینه معتقدند که اصولاً شرکت یا هرشخص حقوقی دیگر فاقد شخصـیتی اسـت کـه بتواند راساً اثر ادبی و هنری خلق کند و امکان و استعداد آن را ندارد که فکر کند، ذوق هنری بکار ببندد، قلم به دسـت گیـرد و اثری را خلق کند تا بتوان آنرا بعنوان خالق اثر محسوب نمود (۱۳) برخی نیز بر این باورند که شناختن عنوان پدیدآورنـده بـرای شخص حقوقی بر خلاف اصل و استثنائی است (۱۴) . بعضی نیز صراحتاً اظهارنظر کرده‌اند که تنهـا انسـانها مـی‌تواننـد مالـک حقوق معنوی باشند. (۱۵) برای تجزیه و تحلیل دقیق این مساله باید گفت که طبق ماده ۵۸۸ قانون تجارت: " شخص حقـوقی می‌تواند دارای کلیه حقوق و تکالیفی شود که قانون برای افراد قائل است مگر حقوق و وظایفی که بالطبیعه فقط انسان ممکـن است دارای آن شود مانند حقوق و وظایف ابوت، بنوت و امثال ذالک "

پس، این ماده قانونی اصلی را تاسیس کرده که بموجب آن شـخص حقـوقی دارای کلیـه حقـوق و وظـایف اشـخاص حقیقی خواهد بود و استثنائاً ممکن است از داشتن برخی حقوق و تکالیف محروم شود و این استثناء علاوه بر اینکه نیاز به اثبات دارد (و باتوجه مثالهای مندرج در متن ماده، اثبات شمول استثناء نسبت به امری در همـان محـدوده قابـل تفسـیر و امکانپـذیر است) مضاف بر این، در هرکجا شک کنیم که ایا شخص حقوقی می‌تواند دارنده حق یا تکلیفی شود یا خیر؟ بایسـتی اسـتثناء را تفسیر مضیق نموده و به قدر متیقن آن اکتفا کرد و به اصل صلاحیت عام شخص حقوقی مراجعه نمود. تردیدی نیست که خود شخص حقوقی راساً نمی‌تواند اثری را خلق کند ولی مگر کدامیک از اعمال حقوقی و یا مادی که به شـخص حقـوقی منتسـب می‌شود را خود شخص حقوقی انجام می‌دهد. اعمالی که از طـرف و بنـام شـخص حقـوقی انجـام مـی‌شـود توسـط اشـخاص حقیقی(مدیران و کارکنان) انجام می‌شود و این اعمال قانوناً و بنابه ماهیت و مکانیسم شخصیت حقـوقی، بـه شـخص حقـوقی

منتسب می‌شود. لذا وقتی که چند نفر در شرکتی دور هم جمع شده و باتلاش دسته جمعی و گروهی (مدیران، کارکنان، تحلیلگر، طراح، برنامه نویس) مبادرت به تولید نرم‌افزاری می‌نمایند، این نرم افزار معلول تلاش و عملکرد دسته جمعی آنهاست که هویت جمعی و گروهی یافته و در شخصیت حقوقی متبلور و مجسم شده است و فی الواقع نمیتوان شخص خاصی را در این میان خالق اثر معرفی کرد. تولید نرم افزار حاصل تلاش همه افراد مذکور است که اگر هرکدام از آنها نباشند، شاید این کار به انجام نرسد. لذا علیرغم نظر برخی(۱۶) در اینگونه موارد نمیتوان صرفاً برنامه نویس را مالک حقوق نرم افزار تلقی نمود پس شخص حقوقی می‌تواند مالک حقوق معنوی و (بالطبع مادی) نرم افزار و در واقع خالق نرم افزار باشد.

۱-٤- موضع قانون حمایت از حقوق پدیدآورندگان نرم افزارهای رایانه ای

قانون در خصوص حقوق معنوی نرم افزار پدید آمده در جریان استخدام قائل به تفکیک شده است. بدین معنی که احکام متفاوتی در مورد حق انتساب اثر به پدیداورنده (right of paternity) و حق پدیدآورنده نسبت به تمامیت اثر (right of integrity) مقرر کرده است. در بند ب ماده ۶ حق تغییر و توسعه نرم افزار را (همانند حقوق مادی) متعلق به کارفرما و استخدام کننده دانسته است. ولی در بند الف همان ماده اشعار می‌دارد که باید نام پدیدآورنده توسط متقاضی ثبت به مراجع یادشده در قانون بمنظور صدور گواهی ثبت اعلام گردد. پس در واقع قانونگذار بین جنبه‌هایی از حقوق معنوی که بیشتر اثر مادی و اقتصادی دارد (تغییر و توسعه نرم افزار) که در عین حال باتوجه به پیشرفت علوم و فنون لزوم انجام آن بمنظور پاسخگویی به نیازهای جدید لازم و ضروری شناخته می‌شود و جنبه دیگری از حقوق معنوی که بیشتر جنبه اخلاقی و فلسفی دارد (انتساب نرم افزار به پدیدآورنده) تمایز قائل شده: حکم اولی را به حکم حقوق مادی الحاق نموده و در مورد دومی حکمی خاص مقرر داشته است. این رویکرد در واقع از یک تمایل شایع در قانونگذاران سرچشمه می‌گیرد که شدیداً و بنحو وسیعی حقوق معنوی را در نرم افزار محدود سازند. (۱۷)

در اینجا ذکر این نکته لازم و ضروری است که قانون یاد شده در ماده ۱ خود حقوق مادی و معنوی را متعلق به پدید آورنده دانسته و در ماده ۶ خود، فقط نسبت به دو مورد از حقوق معنوی یعنی حق انتساب و حق نسبت به تمامیت اثر در خصوص نرم افزارهای پدیدآمده در جریان استخدام تعیین تکلیف نموده است ولی حقوق معنوی را تعریف و منحصر به همین دو مورد نکرده است لذا ممکن است وجود موارد دیگری از حقوق معنوی متصور و قابل فرض باشد چنانچه در برخی کشورها (آلمان، فرانسه،ایتالیا، اسپانیا) حق پس گرفتن و استرداد اثر و در بعضی از کشورها نیز حق افشاء و ابراز اثر (اینکه کی و چگونه اثر از حالت خصوصی خارج گشته و به عموم عرضه شود، به رسمیت شناخته شده است (۱۸) که در فرض ما می‌تواند با حقوق مادی کارفرما تعارض داشته باشد. بهرحال لزوم تعیین دقیق محدوده حقوق معنوی و احصاء موارد آن توسط مقنن ضروری بنظر می‌رسد.

همانگونه که اشاره شد در مورد نرم‌افزارهای پدیدآمده در جریان استخدام با جدائی حقوق مادی و معنوی از یکدیگر و الحاق حکم بخشی از حقوق معنوی پدیدآورنده به حقوق مادی، ظاهراً یک حق برای پدیدآورنده باقی می‌ماند و آن عبارتست از اینکه خالق و پدیدآورنده نرم افزار شناخته شود که این حق نیز صرفاً یک حق و رابطه معنوی و اخلاقی بوده و بهره اقتصادی برای دارنده آن در پی ندارد. آنچه در این میان مهم و اساسی است اینکه مفهوم پدیدآورنده و خالق نرم افزار بدرستی تحلیل و تعریف شود. اشاره نمودیم که از نظر قانونی هیچ اشکالی وجود ندارد که شخص حقوقی (فرضاً یک شرکت نرم افزاری) را

پدیدآورنده نرم افزار تلقی و معرفی کنیم و این یک امر بدیع و دور از ذهنی نیست بلکه باتجزیه و تحلیل فرایند تهیه و تولید نرم افزار میتوان به این نتیجه رسید که در شرکتها این عمل در واقع معلول و نتیجه کارگروهی از افراد است که تحت نام شخص حقوقی گرد هم جمع شده‌اند و در صورتیکه شخص حقوقی در میان نبود، طبعاً این گروه و هویت جمعی حاصل نگردیده و نرم افزاری هم پدید نمی‌آمد. لذا در اینگونه موارد خود شرکت بعنوان پدیدآورنده نرم افزار معرفی و نرم افزار بنام وی ثبت می‌شود. در حقوق فرانسه نیز شخص حقوقی هنگامی پدیدآورنده و مالک اثر شناخته می‌شود که اثر به ابتکار و زیر نظر او بوسیله شخص حقیقی تهیه و بانام شخص حقوقی منتشر شده باشد. (۱۹)

برای حل مشکل جدایی پدیدآورنده اثر از مالک حقوق مادی، در برخی کشورها پذیرفته شده که پدیدآورنده و مالک حقوق معنوی می‌تواند از حقوق معنوی خویش اعراض نماید. این اعراض می‌تواند نسبت به یک اثر باشد یا نسبت به تمامی آثار یک مولف (یا پدیدآورنده). و هچنین اعراض می‌تواند منحصر به آثار موجود باشد یا حتی آثاری که در آینده پدید می‌آیند را نیز در بر بگیرد. ضوابط و مقررات چنین اعراضی تابع قواعد حقوق قراردادهاست و لذا با توجه به اصول کلی می‌تواند مشروط و یا بدون قید و شرط باشد. (۲۰)

و لذا برخی به مالکان کپی رایت در خصوص آثار پدیدآمده در جریان استخدام توصیه می‌کنند که:

۱- از مستخدم تقاضا کنید که یک رضایتنامه کتبی مشعر به اعراض از حقوق معنوی امضاء کند یا اینکه آن را از شرایط قرارداد استخدام قرار دهید.

۲- از پیمانکاران خود که شخص حقیقی هستند، درخواست کنید که یک رضایت کتبی دال بر اعراض از حقوق معنوی امضاء کنند و یا اینکه آن را جزء شروط تعهدات پیمانکاران جدید قرار دهید.

۳- از پیمانکاران خود که شخص حقوقی هستند درخواست کنید که از مستخدمین خود یا پیمانکاران دست دوم، یک رضایت کتبی مشعر به اعراض از حقوق معنوی خود امضاء و تسلیم کنند. (۲۱)

منتهی این بحث از یک منظر دیگر نیز قابل طرح و بررسی است و آن اینکه اعراض شخص از ذکر نام خود بر روی اثر ملازمه‌ای با ذکر نام شخص دیگری (غیر از خالق اثر) بر روی آن ندارد. در اینگونه موارد حقوق معنوی (در قسمت حق انتساب) نرم افزار بدون مالک (بدون ذکر نام مالک) باقی می‌ماند ولی حقوق مادی و بخش دیگری از حقوق معنوی (حق تغییر و توسعه) متعلق به کارفرماست که می‌تواند خود را مالک این بخش از حقوق معرفی و آنها را اعمال کند.

در حقوق ما اعراض، ایقاعی است که سبب قطع رابطه مالکیت بین شخص و مال می‌شود و آن را در زمره اموال مباح در می‌آورد که از طرف اشخاص دیگر قابل تملک است (۲۲) و آنچه که به موضوع بحث ما مربوط می‌شود، در واقع انصراف از حقوق موجود یا آتی است که در بحث اسقاط حق، قابل طرح و بررسی است. برخی یکی از سه اثر اصلی حق را قابلیت اسقاط آن دانسته‌اند منتهی در ادامه یک رشته حقوق خصوصی را قائم به شخص صاحب حق دانسته و غیر قابل اسقاط (و غیر قابل انتقال) معرفی کرده‌اند.(۲۳) اگر پدیدآورنده، حق خود را نسبت به یک اثر موجود اسقاط کند در صحت و درستی آن تردیدی نیست ولی مشکل زمانی است که هنوز نرم افزار تهیه و تولید نشده و اسقاط هرگونه حقی نسبت به آن، ممکن است از مصادیق اسقاط مالم یجب تلقی گردد که در عدم صحت آن شکی نیست. منتهی در حقوق ما حقی (و یا دینی) که سبب آن ایجاد شده نیز به حق (یا دین) موجود الحاق می‌شود لذا اگر در هنگام اسقاط حق، سبب آن ایجاد شده باشد، اسقاط مالم یجب نخواهد بود. در بحث ما اگر بتوان قرارداد منعقده برای تهیه و تولید نرم افزار (که در آن اسقاط حق پدیدآورنده شرط می‌شود) را سبب

حق پدیدآورنده دانست، در هنگام انعقاد قرارداد، سبب آن موجود بوده و لذا اسقاط آن نیز بلااشکال است. مضاف آنکه می‌توان شرط نمود که حق بمحض ایجاد شدن از بین برود و حیات حقوقی نیابد.

۵- نتیجه گیری

۱- قانونگذار ما حقوق مادی نرم‌افزارهای پدیدآمده در جریان استخدام را متعلق به استخدام کننده دانسته است مگر اینکه در قرارداد بنحو دیگری توافق شده باشد.

۲- مقنن در خصوص حقوق معنوی قائل به تفکیک شده است:

الف – حق پدیدآورنده نسبت به انتساب اثر به او متعلق به پدیدآورنده است.

ب – حق نسبت به تمامیت اثر (در قسمت تغییر و توسعه آن) تابع احکام حقوق مادی و متعلق به کارفرماست.

۳- شخص حقوقی می‌تواند بعنوان پدیدآورنده اثر و مالک حقوق معنوی شناخته شود. لذا اگر پدیدآمدن نرم افزار معلول تلاش برخی اشخاص حقیقی تحت نام و عنوان شخص حقوقی باشد، بگونه‌ای که نتوان پدیدآمدن نرم افزار را مشخصاً به یکی از افراد منتسب ساخت، شخص حقوقی مالک حقوق معنوی نرم افزار است.

۴- اشخاصی که برای پدیدآوردن نرم افزار استخدام می‌شوند، می‌توانند مبادرت به اسقاط حقوق فعلی و یا آتی خود نسبت به حقوق معنوی نرم‌افزار نمایند. در اینصورت بخشی از حقوق معنوی نرم افزار (حق انتساب) بدون مالک و بدون عنوان باقی می‌ماند و کارفرما، مالک حقوق مادی و بخش دیگری از حقوق معنوی (حق تغییر وتوسعه) می‌باشد.

پی نوشتها:

۱- دکتر سید عزت ا.. عراقی – *حقوق کار* – انتشارات سمت – تهران ۱۳۸۱ ص ۱۶۵تا ۱۶۷

2-Tina Hart&Linda Fazzani-*intellectual property law*-palgrave Macmillan-Great Britain-third edition-2004-page149-153&165

۳- دکتر امیر صادقی نشاط- *حمایت از حقوق پدیدآورندگان نرم افزارهای رایانه‌ای* – شورایعالی انفورماتیک ، سازمان برنامه و بودجه – تهران ۱۳۶۷- ص ۹۱

4-Tina Hart&Linda fazzani-op.cit-page 193

5-ibid-page 197 and Dr Uma Suthersanen&Dr Makeen Makeen –Author s moral right in uk and china –page 15- *www.chinaiprlaw.com*"

۶- دکتر امیر صادقی نشاط-همان-ص ۹۵

7-Tina Hart & Linda Fazzani –op.cit-page 193

8-moral right and author 's rights –*www.elj.wawick.ac.uk/jilt*

۹- برای ملاحظه متن انگلیسی کنوانسیون برن و متن انگلیسی و فارسی موافقتنامه trips رک به سایت شرکت همکاران سیستم *www.systemgroup.net* صفحه حقوق فناوری اطلاعات-بخش قوانین و مقررات

10-*www.elj.warwick.ac.uk/jilt*.opcit

۱۱- دکتر امیر صادقی نشاط-همان-ص ۱۲۷

۱۲- پیشین- -ص۹۱

۱۳- همان- -ص ۹۶و۹۷و۱۰۰

۱۴- علیرضا نوروزی- *حقوق مالکیت فکری- حق مولف و مالکیت صنعتی* – نشر چاپار – تهران ۱۳۸۱ -ص۵۹و۶۰

15-Adam Gamble&Mark Sallis-moral right in copyright work-*www.arcuslegal.com.au*

16-software copyright and the computer programmer-www.ipr-helpdesk.org/docs

17-ibid

18-*www.elj.warwick.ac.uk/jilt*-op.cit

۱۹- علیرضا نوروزی-همان-ص ۶۰-۵۹

20-*T*ina Hart & Linda Fazzani-op.cit-page 197 and *www.elj.wawick.ac.uk/jilt*-op.cit-Dr" Suthersanen&Dr Makeen Makeen-op.cit-

21-*A*dam Gamble &Mark Sallis-op.cit

۲۲- دکتر ناصر کاتوزیان – *حقوق مدنی، ایقاع* – نشر یلدا – تهران – ۱۳۷۰ ص ۸۶، ش ۴۱ – همچنین دکتر محمد جعفر جعفری لنگرودی – *ترمینولوژی حقوق* – کتابخانه گنج دانش – تهران ۱۳۶۸- ص ۶۳ ش ۴۸۰.

۲۳- دکتر محمد جعفر جعفری لنگرودی – حقوق اسلام – کتابخانه گنج دانش- تهران – ۱۳۷۰ – ص ۵ – ش ۲/۱ و ص ۹ ش ۷/۱

☑ عنوان: اصول حاکم بر حمایت از داده

☑ نویسنده: حمیدرضا اصلانی (دانشجوی دکترای حقوق خصوصی دانشگاه شهید بهشتی)

چکیده

مراد از اصول حاکم بر حمایت از داده، آموزه‌های کلی حقوقی است که راهنمای قانونگذار در تدوین قوانین و قضات در رسیدگی‌های قضایی می‌باشد. این اصول با توجه به مراحل مختلف انجام عملیات بر روی داده‌های شخصی قابل تقسیم‌بندی و بررسی می‌باشند. تحلیل این اصول می‌تواند ما را در تهیه قوانین مناسب و جامع یاری نموده و در مقام رسیدگی قضایی، در موارد اجمال یا ابهام یا سکوت قوانین رهاننده دادرس از سرگردانی باشد.

کلمات کلیدی: حریم خصوصی، حمایت از داده، اصل، اصول حاکم بر حمایت از داده.

۱- مقدمه

مراد از اصول حاکم بر حمایت از داده یا حریم خصوصی اطلاعاتی[۱](INFORMATION PRIVACY) قواعد کلی است که حاکم بر موضوع حمایت از داده بوده و می‌توان با یاری جستن از آنها حتی در مواردی که قانونگذار حکم صریح و خاصی ندارد در تبیین و تعیین فروع بحث و یافتن راه‌حل‌های مسائل و قضایای جزئی به راه‌حل قضیه دست یافت. لذا باید گفت که این اصول دارای کارکردی دوگانه می‌باشند: **ازیکسو** مبین رهیافت و رویکرد مورد اتخاذ قانون‌گذاران مختلف بوده و رعایت یا عدم رعایت آنها در تدوین قوانین و مقررات مربوط، نشانگر جهت‌گیری کلی حاکم بر تقنین است و **از سوی دیگر** در مقام تفسیر مواد قانون در موارد ابهام یا اجمال یا تعارض این مواد با یکدیگر راهنمای حقوقدانان و محاکم در جهت یافتن راه حل نهایی هر قضیه می‌باشد.

ذیلاً اهم اصول حاکم بر حمایت از داده را در پنج بند تقسیم‌بندی نموده و اشاره‌ای مختصر به مفهوم هریک خواهیم داشت. لازم به یادآوری است که در تدوین این اصول نظام حقوقی خاصی مدنظر نبوده است بلکه سعی شده تا با استقراء در نظام‌های حقوقی مختلف و اسناد بین‌المللی معتبر اهم این اصول استخراج شده و با یک دسته‌بندی جدید عرضه شوند. لذا علیرغم آنکه اغلب اصول مزبور در نظام‌های مختلف حقوقی مورد پذیرش واقع شده اند معهذا احتمال فقدان یک یا برخی از آنها در هریک از نظام‌های حقوقی وجود دارد[۱]. علت تقسیم این اصول ذیل پنج عنوان آنست که مراحل چهارگانه تحصیل، نگهداری، بکارگیری و انتقال یا امحاء داده‌ها چهار مرحله اصلی قابل تصور در طول حیات داده‌ها می‌باشند که هریک اصول خاص خود را دارند و در کنار این چهار دسته، اصولی نیز وجود دارند که حاکم بر کل پروسه، بوده و اختصاص به یک فاز ندارند که آنها را

۱- برخی از این اصول را می‌توان در ماده ۶ دستورالعمل شماره **95/46/EC** اتحادیه اروپایی یافت.ر.ک[۲]

تحت عنوان سایر اصول در عرض چهار دسته پیش‌گفته بررسی خواهیم نمود. لذا همانگونه که ملاحظه می‌شود این اصول به پنج دسته به شرح ذیل قابل انقسامند.

- **اصول مربوط به تحصیل داده‌ها**
- **اصول مربوط به نگهداری داده‌ها**
- **اصول مربوط به بکارگیری داده‌ها**
- **اصول مربوط به امحاء و انتقال داده‌ها**
- **سایر اصول**

۲- اصول مربوط به تحصیل داده‌ها:

ویژگی این دسته از اصول آنست که علی‌الاصول ناظر بر مرحله گردآوری و تحصیل داده‌ها می‌باشند. این اصول تحت چهار عنوان به شرح ذیل قابل بررسی می‌باشند:

۲-۱- اصل تحصیل قانونی و منصفانه[۲](Fair and Lawfull Collection):

این اصل ناظر بر روش و ابزار مورد استفاده در تحصیل داده‌هاست. مطابق این اصل تحصیل داده‌های شخصی مربوط به دیگری می‌باید از طریق روش و ابزار قانونی و مشروع صورت گیرد. اگر تعبیر دقیق‌تری از این اصل مدنظر باشد می‌توان گفت که مطابق این اصل توسل به ابزار یا روش غیرقانونی و غیرمنصفانه برای گردآوری داده‌ها ممنوع است. لذا تحصیل این گونه داده‌ها در درجه اول با رضایت شخص سوژه و در صورت فقدان چنین رضایتی، تنها بنا بر حکم صریح قانونگذار آنهم در موارد خاص و استثنایی مصرح مجاز می‌باشد. در نتیجه تحصیل داده‌ها بصورت سری و محرمانه علی‌الاصول ممنوع است (**اصل اطلاع**). البته پر واضح است که این اصل نیز همچون همه اصول مطلق و بدون استثناء باقی نمانده[۳] و در موارد خاصی با اجازه خاص قانونگذار و در حدود چنین اجازه‌ای می‌توان از آن دست شست (که از آن جمله می‌توان به موارد امنیتی و حفظ مصالح حیاتی جامعه اشاره کرد).

۲-۲- اصل تحصیل مضیق و مرتبط[۴](Collection for a proper purpose)

اصل تحصیل قانونی و منصفانه ناظر بر ابزار و روش مورد استفاده در تحصیل داده‌ها بود. لیکن این اصل ناظر بر نوع و میزان داده‌ها گردآوری شده می‌باشد. بموجب این اصل **اولاً** تحصیل داده‌ها تنها برای هدف قانونی و مشروع مجاز است (یا لااقل می‌توان گفت تحصیل داده‌ها برای هدف غیر قانونی یا نامشروع ممنوع است). **ثانیاً** نوع داده‌های گردآوری شده باید با هدف اولیه تحصیل داده‌ها منطبق باشد **ثالثاً** گردآوری داده‌ها باید تنها به میزان مورد نیاز برای هدف اولیه و اعلام شده صورت گیرد و گردآوری داده‌های اضافی ممنوع است. بر این اساس به عنوان مثال مؤسسه‌ای که در زمینه نرم‌افزارهای کامپیوتری فعالیت

---

۲ – در برخی منابع از این اصل تحت عنوان منصفانه بودن روش گردآوری داده (Fair means of collection)یاد شده است. به عنوان نمونه ر.ک:[۳]

۳- ما من عامٍ الا و قد خص

۴- در برخی منابع از این اصل با عنوان اصل هدف مضیق (Purpose Limitation Principle)یاد شده است. به عنوان نمونه ر.ک:[۳]

می‌کند و برای اطلاع از سلایق و خصوصیات مشتریان خود با جلب رضایت آنها اقدام به گردآوری داده‌هایشان می‌نماید نمی‌تواند انتظار داشته باشد که گردآوری داده‌های مربوط به بیماری‌های مسری مشتریانش نیز بموجب رضایت اخذ شده از مشتریان مشروع تلقی شود.

۲-۳- اصل انتخاب(Opt Principle)

اصل انتخاب بدان معناست که مؤسسه یا شخصی که قصد گردآوری داده‌ها در خصوص شخص سوژه را دارد پیش از هرچیز می‌باید این امکان را برای کاربر فراهم آورد که صریحاً نظر خود را مبنی بر اینکه آیا با گردآوری داده‌های شخصی خود موافقت دارد یا خیر؟ اعلام نماید. این عمل از طریق یک روش انتخاب صورت می‌گیرد که ممکن است مبتنی بر روش سلبی (Opt-out)بوده یا از طریق روش ایجابی(Opt-in) صورت گیرد.

در روش سلبی کاربر در بدو ورود می‌تواند نظرش را مبنی بر مخالفت با تحصیل داده‌های شخصی خود، اعلام داشته و از این طریق از گردآوری داده‌ها جلوگیری کند و در صورتی که مخالفت خود را اعلام ننماید (سکوت کند) این امر بمنزله اعلام موافقت تلقی شده و تحصیل داده‌ها مجاز تلقی خواهد شد. برعکس روش فوق در روش ایجابی که از حیث دلالت قطعی بر اراده کاربر از اطمینان بیشتری برخوردار است، در بدو ورود کاربر به سایت از او خواسته می‌شود که موافقت خود را با گردآوری داده‌های خود (که ممکن است تمام یا بخشی از ما به ازای دریافت خدمات سایت باشد) اعلام دارد. در چنین فرضی سکوت کاربر (عدم اعلام موافقت) بمنزله مخالفت تلقی شده و تحصیل داده‌ها ممنوع خواهد بود[۴].

نکته مهم در خصوص اصل انتخاب رعایت بموقع و صحیح تکلیف دارنده سایت دائر بر اعلام حق انتخاب کاربر به وی می‌باشد. از این جهت، ضروری است که اعمال حق انتخاب توسط کاربر پیش از هرگونه گردآوری داده‌ها صورت پذیرفته باشد و لذا ارائه این گزینه‌ها (موافقت یا مخالفت) در اثنای استفاده کاربر از سایت (که ممکن است پیش از آن بخشی از داده‌های او تحصیل شده باشد) نمی‌تواند تضمین کننده رعایت این اصل بوده و مآلاً داده‌های اخذ شده پیش از اعلان رضایت کاربر (و به طریق اولی پس از اعلام مخالفت او) تحصیل شده از طریق غیر مجاز تلقی می‌شوند. همچنین اعلام این گزینه‌ها از سوی سایت به کاربر باید به گونه‌ای باشد که بتوان یقین حاصل نمود که یک کاربر معمولی، در شرایط معقول، قطعاً با آن مواجه شده و متوجه آن خواهد شد و لذا ارائه آنها به نحوی که کاربر ناگزیر از دیدن آنها باشد (مثلاً مجوز ادامه فعالیت کاربر باشد) تضمین‌کننده حسن اجرای این اصل است. البته یکی از مشکلات موجود در مسیر رعایت این اصل آن است که کاربران همیشه از مجرای ورودی سایت وارد آن نمی‌شوند و ممکن است که کاربری از طریق پیوندی(LINK)میان یک صفحه از سایت (WEBPAGE) با صفحه‌ای از سایت دیگر اقدام به ورود به صفحات میانی سایت نماید که در این صورت مشکل اعلام گزینه‌ها مسأله‌ای بغرنج می‌شود.

۲-٤- اصل اطلاع(NOTICE PRINCIPLE) [۵]:

۵- اصطلاح معادل دیگری که در این خصوص مورد استفاده قرار می‌گیرد و رواج دارد "**آگاه کردن کاربر از دلیل گردآوری داده‌ها** " (Informing users why information is collected) می‌باشد که البته تنها ناظر بر مرحله گردآوری داده‌هاست و نسبت به مرحله پردازش داده‌ها شمولی ندارد. ر.ک:[۳]همچنین در برخی متون اصلاح **اصل آگاهی**(Awareness Principle) به همین مفهوم بکار رفته است.ر.ک: [۵]

همچنین در برخی متون از اصطلاح مشارکت شخص سوژه (Individual Participation) استفاده شده است.ر.ک:[۶]

همانگونه که پیشتر دیدیم اصل تحصیل قانونی و منصفانه اقتضای آن دارد که گردآوری داده‌ها از طریق روش‌ها و ابزارهـای غیرقانونی و نامشروع ممنوع باشد. همچنین گفته شد که بر این مبنا گردآوری داده‌ها بصورت سری و محرمانه ممنوع می‌باشـد. از این رو می‌توان اصل اطلاع را از توابع و فروع اصل تحصیل قانونی و منصفانه تلقی نمود. لیکن دلیـل بررسـی مسـتقل ایـن اصل در اینجا آنست که:

اولاً: هرچند این اصل از فروع اصل پیش گفته محسوب می‌شود لیکن مدلول اصل تحصیل قانونی و منصـفانه بـه خـودی خود دلالت صریحی لزوم اطلاع‌رسانی و ابلاغ مسأله گردآوری داده‌ها نداشته و بدون تصریح به اصل اطلاع ممکـن اسـت ایـن شبهه ایجاد گردد که مراد از اصل تحصیل قانونی و منصفانه تنها فقدان ممنوعیت قانونی در مرحله بدست آوردن داده‌ها اسـت و مآلاً نسبت به اطلاع‌رسانی به سوژه که امری است علیحده، تکلیفی وجود ندارد.

ثانیاً: هرچند اصل اطلاع به دلیل تقدم تحصیل داده‌ها بر پردازش داده‌ها در زمره اصول حاکم بر تحصیل داده‌ها برشـمرده شده است لیکن واقعیت آن است که این اصل علاوه بر اینکه در مرحله تحصیل داده‌ها لازم الرعایه می‌باشـد بعضـاً در مرحلـه پردازش داده‌ها نیز حکومت دارد (بویژه در موارد اصلاح یا تغییر دادن داده‌ها) و ذکر این اصل در زمره اصول حاکم بـر تحصـیل داده‌ها تنها به این دلیل است که این مرحله منطقاً مقدم بر پردازش داده‌هاست و برای پرهیز از تکرار مکررات هردو بحث ذیـل یک عنوان بررسی می‌شود. لذا اصل تحصیل قانونی و منصفانه که صرفاً ناظر بر مرحله اول است حتی اگـر دلالـت ضـمنی بـر لزوم اطلاع‌رسانی در مرحله تحصیل داده‌ها داشته باشد شامل لزوم اطلاع‌رسانی در مرحله پردازش داده‌ها نمـی‌شـود. در نتیجـه بررسی مستقل این دو اصل توجیه پذیر است.

علاوه بر اینکه اصل اطلاع به معنی لزوم اعلام تحصیل داده می‌باشد، اصل مزبور همچنین به مفهوم لزوم اعلام رویه مـورد عمل یک سایت در خصوص نحوه حمایت از حریم خصوصی کاربران(PRIVACY POLICY) آنهم در بدو ورود کاربر بـه سایت نیز می‌باشد[۴]. از سوی دیگر بر مبنای این اصل اعلام هویت مؤسسه یا شخصـی کـه اطلاعـات را گـردآوری کـرده و هویت پردازشگر داده‌ها، دلیل گردآوری و پردازش داده‌ها، آثار خودداری از ارائه یا باز پس‌گیری داده‌ها و حقوق سوژه در پیگرد و تعقیب مؤسسه، به سوژه ضروری است[۵].

با توضیحات فوق می‌توان گفت که مفهوم اصل اطلاع آنست که گردآوری و پردازش داده‌های شخصی (حداقل در خصوص پردازش‌های تغییر دهنده داده) منوط به اعلام مراتب به شخص سوژه می‌باشد مگر در مواردی که قانون بنا به پـاره‌ای مصـالح استثنایی و مصرح (همچون مسائل امنیتی) خلاف آن را مقرر دارد[۷].

لازم به ذکر است که برخی، دو اصل **تحصیل قانونی و منصفانه** و **اطلاع** را تحت عنوان اصل **محدودیت تحصـیل داده** (Data Collection Limitation) بررسی نموده‌اند[۶].

۳- اصول مربوط به نگهداری داده‌ها

در این دسته اصولی جای می‌گیرند که بیش از هرچیز ناظر بر مرحله نگهداری داده‌ها توسط پردازشگر می‌باشند. این اصول در چهار بند به شرح ذیل قابل بررسی می‌باشند:

۳-۱- اصل امنیت(Security Principle)

اصل امنیت بدان معناست که کسی که داده‌ها را تحصیل نموده یا در اختیار دارد می‌باید تدابیر امنیتی لازم برای جلوگیری از دسترسی یا پردازش غیر مجاز داده‌ها توسط دیگران بکار گیرد[۳] و عدم بکار گیری چنین تدابیری موجب مسؤولیت اوست.این اصل بویژه ناظر بر دارندگان مؤسسات خدمات اینترنتی نظیرISP ها می‌باشد.البته مسؤولیت این قبیل اشخاص منافاتی با مسؤولیت شخصی که بصورت غیر مجاز اقدام به ورود یا تحصیل یا پردازش و یا انتشار داده‌های مزبور نموده است ندارد و ممکن است سوژه بموجب این اصل علیه مدیر یک سایت و همزمان بموجب اصل ممنوعیت پردازش غیرمجاز علیه شخص خاطی اقامه دعوا نماید.

از آنجا که نگهداری داده‌ها در موارد غیر ضروری و برای مدت طولانی خود بالقوه خطر دسترسی و پردازش غیرمجاز را افزایش می‌دهد و امحاء داده‌ها در چنین مواردی بهترین راه تضمین امنیت داده است لذا از جمله آثار اصل امنیت، **اصل امحاء** است[۸]که بزودی بدان خواهیم پرداخت.

۳-۲- اصل شفافیت[۶](Transparency Principle)

همانگونه که در جامعه واقعی جرم و تخلف در خفا بیش از علن رخ می‌دهد و علنی شدن فعالیت‌ها در کاهش جرائم مؤثر است، در فضای مجازی نیز علنی کردن فعالیت‌ها می‌تواند به کاهش تخلفات کمک کند. یکی از بهترین روش‌های کنترل در ایفای وظایفی که شخص یا مؤسسه گردآوردنده یا پردازش‌کننده داده‌ها برعهده دارد الزام ایشان به شفاف‌سازی و عرضه اطلاعات مربوط به فعالیت‌هایشان است. در صورتی که چنین شخص یا مؤسسه‌ای ملزم باشد که اطلاعات مربوط به داده‌های گردآوری و پردازش شده را بصورت کامل و دائم در دسترس شخص سوژه یا مقام‌های ناظر (نظیر کمیسونر یا کنترل‌گر) قرار دهد همواره خواهد کوشید که از تعدی به حقوق سوژه خودداری نماید.

البته اعمال این اصل نباید به سایر اصول حاکم بر پردازش داده‌ها بویژه اصل امنیت خدشه‌ای وارد کند و عرضه اطلاعات مربوط نباید به گونه‌ای باشد که موجبات وقوف سایرین را به محتوای پایگاه‌های داده فراهم آورد.

بر اساس این اصل مؤسسه مورد بحث باید **اولاً** در صورت تقاضا (on request)، امکان دسترسی اشخاص به محتوا، نوع، هدف گردآوری و سایر اطلاعات مربوط به داده‌های شخصی ایشان را فراهم آورده؛ **ثانیاً** باید رویه خاصی برای حمایت از حریم خصوصی اطلاعاتی اشخاص (Privacy Policy) داشته و آن را بنحو شفاف در دسترس کاربران قرار دهد[۹و۱۰]. در زمینه **داده‌های شخصی حساس** (sensitive personal data) مؤسسه باید اطلاعات مشابه را به مقام ناظر نیز ارائه کند.

۳-۳- اصل دسترسی(Access Principle)

بموجب این اصل که در واقع خود از آثار اصل شفافیت است، مؤسسه دارنده داده‌ها می‌باید در صورت درخواست کاربری که داده‌های او تحصیل یا پردازش می‌شود (سوژه) امکان دستیابی او را به اطلاعات مربوط به نوع، ماهیت و روش گردآوری و احیاناً کیفیت داده‌های مزبور فراهم آورد. در این راستا روش و هزینه اعمال چنین حقی از جانب سوژه نباید به گونه‌ای باشد که عملاً آن را ناممکن یا نامعقول جلوه دهد. همچنین سوژه علاوه بر حق دسترسی به این اطلاعات حق کپی‌برداری و همچنین اطلاع از هویت مؤسسات و اشخاصی که داده‌ها در اختیار ایشان قرار گرفته است را دارد[۱۲و۱۳].

مع‌الوصف اعمال این اصل در موارد ذیل ممکن است با محدودیت‌ها و استثناهایی مواجه شود:

۶- در برخی متون اصطلاح **اصل گشوده بودن(Openness Principle)**به همین مفهوم بکار رفته است.ر.ک:[۸]

- وقتی که دسترسی موجب ایجاد ناامنی یا خطر برای سلامتی یا حیات دیگری باشد؛
- وقتی که دسترسی موجب ایجاد خطر یا تهدید جدی برای حریم خصوصی سایرین باشد؛
- وقتی که درخواست دسترسی با توجه به اوضاع و احوال فاقد توجیه منطقی بوده و صرفاً به منظور آزار و اخلال باشد؛
- وقتی که داده‌ها مربوط به دعوای جاری میان سوژه و مؤسسه نزد مراجع قانونی بوده و بموجب مقررات حاکم بر مرجع رسیدگی دسترسی بدانها امکانپذیر نباشد؛
- وقتی که منع دسترسی بموجب حکم قانون باشد؛
- وقتی که منع دسترسی بموجب حکم مقام صلاحیتدار (قضایی– امنیتی) باشد؛
- وقتی که دسترسی موجب اخلال در تعقیب و کشف یک جرم مهم باشد[۹و۱۴]؛

۳-٤- اصل صحت[۷] (Accuracy of Information)

عدم صحت داده‌ها همواره خطری بالقوه برای حریم خصوصی اشخاص محسوب می‌شود. دلیل عدم صحت داده‌ها ممکن است اشتباه یا قصور در مرحله گردآوری داده‌ها یا ذخیره داده‌ها یا پردازش داده‌ها باشد و یا کامل نبودن داده‌های گردآوری شده موجب عدم انطباق آنها با واقع باشد، یا اینکه داده‌های مورد بحث در مراحل فوق بنو صحیح گردآوری و ذخیره و پردازش شده لیکن بعدها به دلیل تغییر در مختصات سوژه، عدم انطباق داده‌ها با واقع مدلل گردد (اصطلاحاً روزآمد نباشند) و نیاز به اصلاح داشته باشند[۱۵].

در هرحال اصل صحت داده‌ها که اصلی کیفی بوده و ناظر بر محتوای داده‌ها است اقتضای آن دارد که مؤسسه یا شخصی که به گردآوری و پردازش داده‌ها می‌پردازد در تمام مراحل، نه تنها داده‌های صحیح گردآوری پردازش و منتقل نماید بلکه ترتیبات و تدابیر مقتضی برای حصول اطمینان از صحیح بودن، کامل بودن و روزآمد بودن داده‌ها نیز بکار گیرد. از نتایج اصل صحت داده‌ها آنست که در صورتی که شخص سوژه تقاضای اصلاح داده‌ها برای منطبق شدن آنها با واقع را نماید شخص یا مؤسسه مورد بحث مکلف است ضمن بررسی وضعیت داده‌ها و ادعای سوژه، در صورتی که ادعای سوژه مقرون به صحت باشد نسبت به اصلاح داده‌ها اقدام نماید و الا مسؤول خواهد بود.

٤- اصول مربوط به بکار گیری داده‌ها

این اصول علی‌القاعده ناظر بر چگونگی بکارگیری داده‌ها و بهره‌برداری از آنها می‌باشند و در دو بند به شرح ذیل قابل بررسی می‌باشند:

٤-۱- اصل پردازش مرتبط[۸] (proper purpose proccess)

۷- از این اصل با عنوان کیفیت داده‌ها(Data Quality) یا کیفیت اطلاعات(Information Quality) نیز یاد شده است.ر.ک: [۱۵و۵و۱۴و۶]

۸- در برخی منابع از این اصل با عنوان اصل محدودیت استعمال **(Use Limitation Principle)** یاد شده است. بعنوان نمونه ر.ک:[۶]

اصل ممنوعیت پردازش داده‌های شخصی مقتضی است که گردآورنده و پردازشگر تنها اجازه پردازش داده‌ها را در حدود مورد توافق داشته یا آنکه قانونگذار چنین اجازه‌ای را بوی داده باشد و از پردازش آنها برای اهداف غیرمرتبط و ثانوی (secondary purpose)خودداری کند. لذا **اولاً** چنین شخصی باید از پردازش داده‌ها در مواردی غیر از دو فرض فوق خودداری نماید **ثانیاً**در صورت تردید در روا بودن یا نبودن پردازش اصل مجاز نبودن آنست مگر اینکه صریحاً مجوزی برای آن وجود داشته باشد. عدم رعایت هریک از موارد فوق می‌تواند برای پردازشگر مسؤولیت ببار آورد.

با این همه در مواردی که هدف ثانوی از لوازم و فروع منطقی و غیرقابل اجتناب هدف اولیه باشد یا آنکه سوژه منطقا انتظار چنین پردازشی را داشته باشد، بجز در خصوص داده‌های شخصی حساس، چنین پردازشی مجاز است. در هر حال در خصوص اطلاعات مربوط به سلامتی و بطور کلی داده‌های شخصی حساس مقررات مفصلی وجود دارد که جملگی از فروع این بحث می‌باشند و بررسی آنها در این مختصر نمی‌گنجد و برای مطالعه آنها باید به منابع مفصل‌تر مراجعه نمود[۱۶].

٤-۲- اصل ممنوعیت افشاء[۹] (Disclosure Restriction Principle)

گردآوری و پردازش همانگونه که پیشتر اشاره شد محدود به هدفی است که تفسیر موسع آن در هرحال ممنوع بوده و تسری دادن آن به موارد مشابه تجاوز به حریم خصوصی اطلاعاتی محسوب می‌شود. خواه سوژه خود داده‌های شخصی را در اختیار پردازشگر قرار داده باشد یا آنکه پردازشگر از سایر طرق قانونی و به طریق اولی غیر قانونی آنها را به دست آورده باشد افشاء داده‌ها به اشخاص ثالث و بمنظور نیل به یک هدف ثانوی، امری است که علی‌الاصول در چارچوب اجازه اولیه صادره از سوی سوژه یا قانونگذار نمی‌گنجد و لذا ممنوع است و این اصل در تمامی مراحل تحصیل پردازش و انتقال داده‌ها لازم‌الرعایه می‌باشد.

با اینحال در موارد ذیل افشاء داده‌ها به اشخاص ثالث و برای هدف ثانوی مجاز است:

- وقتی که هدف ثانوی ارتباط تامی با هدف اولیه گردآوری داده‌ها داشته و سوژه نیز منطقاً انتظار افشاء داده‌ها برای چنین منظوری را داشته باشد، مگر درخصوص داده‌های شخصی حساس که این امر در هرحال ممنوع است؛
- وقتی شخص سوژه رضایت دهد؛
- وقتی مؤسسه یا شخص دارنده داده‌ها بنحو معقولی اعتقاد دارد که افشاء داده‌ها برای صیانت از سلامتی یا حیات سوژه و یا امنیت و سلامت عمومی ضرورت دارد؛
- وقتی که افشاء داده‌ها برای تحقیقات پزشکی ضروری باشد (با رعایت شرایط و قیود خاص)؛
- وقتی که افشاء داده‌ها برای جلوگیری از وقوع یک جرم مهم ضروری باشد؛
- وقتی که افشاء داده‌ها بموجب حکم قانون ضروری باشد؛
- وقتی که افشاء داده‌ها بنا به حکم مقام صلاحیتدار (قضایی- امنیتی) ضرورت داشته باشد؛

در خصوص داده‌های شخصی حساس این استثناً تابع مقررات خاص و شدیدتری است که بررسی همه آنها از حوصله این مقال بیرون است[۱۶].

۹- در برخی منابع این اصل ذیل **اصل پردازش مرتبط (اصل محدودیت استعمال)** مطرح شده است.ر.ک[۱۴]

لازم به ذکر است که افشاء داده‌ها با انتقال داده‌ها تفاوت ماهوی دارد و هر چند هر دو عمل علی‌الاصول ممنوع‌اند لیکن افشاء داده‌ها بمعنی فراهم نمودن وضعیتی است که شخص ثالثی بالقوه یا بالفعل امکان وقوف بر آنها را داشته باشد لیکن مراد از انتقال داده‌ها آن است که داده‌ها در اختیار شخص دیگری قرار داده شود و او خود امکان پردازش یا افشاء یا انتقال داده‌ها را بیابد.

۵- اصول مربوط به امحاء و انتقال داده‌ها

پس از گردآوری، نگهداری، و استفاده از داده‌ها نوبت به انتقال و امحاء داده‌ها می‌رسد. ذیلاً اصول حاکم بر این مرحله را در دو بند مورد بررسی قرار می‌دهیم:

۵-۱- اصل امحاء (ERASE PRINCIPLE)

اصل امنیت که از اصول حاکم بر نگهداری داده‌ها می‌باشد را پیشتر مورد بررسی قرار دادیم و گفتیم که لزوم اتخاذ تدابیر امنیتی از جانب دارنده داده‌ها اقتضا دارد بمحض برطرف شدن نیاز وی به داده‌ها نسبت به زائل نمودن و امحاء آنها اقدام نماید. این وظیفه بویژه ناظر بر دارندگان مؤسسات خدمات اینترنتی نظیرISP ها می‌باشد زیرا داده‌های مربوط به کاربران همه روزه در حافظه رایانه‌های این مؤسسات ذخیره می‌شود و پس از نگهداری این داده‌ها برای مدت معقولی که مبتنی توجیهات امنیتی، اقتصادی و احیاناً آماری است ضروری است که این داده‌ها امحاء شوند تا کسی نتواند با دسترسی به داده‌ها از آنها سوء استفاده نماید.

لازم به ذکر است که از آنجا که همانگونه که اشاره شد اصل امحاء از آثار اصل امنیت می‌باشد لذا در اغلب منابع بطور مستقل به این اصل پرداخته نشده و آن را ذیل همان اصل مادر (امنیت) مطرح نموده‌اند[۸ و۱۷] لیکن به دلیل آنکه در نوشتار حاضر سعی شده که اصول مربوط به داده با توجه به مراحل مختلف کار دسته‌بندی شوند لذا این اصل که ناظر بر مرحله امحاء و انتقال داده‌ها است جدا از اصل امنیت که ناظر بر مرحله نگهداری داده‌ها است مطرح شده است.

۵-۲- اصل عدم انتقال[۱٤](Onward Transfer)

خصیصه فرامرزی و گیتی گستر بودن اینترنت و بطور کلی فناوری‌های اطلاعات و ارتباطات این امکان را فراهم آورده که اشخاص بتوانند از این ویژگی برای فرار از مقررات یک نظام حقوقی و یا تعقیب دستگاه‌های قضایی و امنیتی سوء استفاده کنند. به عنوان مثال اگر عملی در یک نظام حقوقی جرم بوده و مستوجب مجازات باشد بر اساس اصل اولیه سرزمینی بودن قوانین کیفری (و در صورت فقدان مجوز قانونی خاص) نمی‌توان بر اساس چنین قانونی حکم به مجرمیت شخصی که در خارج از قلمرو نظام حقوقی مزبور عمل مورد بحث را مرتکب شده باشد داد.

این ویژگی و خصیصه **فاوا** وقتی در کنار مشکل فقدان همگونی و هماهنگی تام میان مقررات نظام‌های مختلف حقوقی قرار می‌گیرد، بویژه در بحث حمایت از داده‌ها اهمیت مضاعف می‌یابد. فرض کنیم که پردازش و افشاء (و نه انتقال) داده‌های شخصی شهروندان در کشور **الف** ممنوع بوده ولی در کشور **ب** حکم مشابهی وجود ندارد. در چنین وضعیتی اگر شخصی با تحصیل داده‌های شخص دیگر در کشور **الف** آنها را از طریق رایانامه (e-mail) برای دوست خود که در کشور **ب** سکونت دارد ارسال می‌نماید و از او می‌خواهد که داده‌ها را از طریق یک وبلاگ یا سایت اختصاصی خود منتشر نماید.

در این مثال کسی تردیدی نخواهد داشت که نتیجه حاصل با فرضی که ارسال کننده داده‌ها خود اقدام به افشاء و انتشار آنها می‌نمود هیچ تفاوتی ندارد و حریم خصوصی شخص سوژه در هر دو فرض به یک اندازه مورد تعدی و تجاوز قرار گرفته است.

بر این اساس در بحث از حریم خصوصی اطلاعاتی یکی از اصول حاکم و بنیادین که در تمام مراحل، باید از سوی دارنده و پردازشگر داده‌ها رعایت شود اصل ممنوعیت انتقال فرامرزی داده (Transborder data flow) است. اهمیت این اصل تابدانجاست که بدون آن در مقام حمایت از داده نقض غرض حاصل می‌شود. برخی کشورها (که عمدتاً در زمره کشورهای تولید کننده داده‌ها و اطلاعات می‌باشند) نظیر کشورهای اروپایی انتقال داده‌ها به کشورهای فاقد سطح کافی حمایت از داده را ممنوع نموده‌اند تا جائی که حتی ایالات متحده امریکا برای پاسخ به نیاز مؤسسات این کشور (که از دید اروپائیان فاقد سطح کافی حمایت از داده است) به مبادله اطلاعات و داده‌ها با همتایان اروپایی خود ناگزیر از تدوین موافقت‌نامه بندرگاه امن (Safe Harbor Agreement) با اروپائیان شد. [۱۸]

البته اصل منع انتقال فرامرزی داده‌ها همچون سایر اصول پیشین دارای استثنائاتی است که بررسی همه آنها از حوصله این مقال بیرون است و برای دیدن آنها باید به منابع مفصل‌تر مراجعه نمود [۸ و۱۹].

۶- سایر اصول

مراد از این عنوان اصولی است که نمی‌توان آنها را مختص یک یا چند مرحله از روند گردآوری، پردازش و امحاء وانتقال داده‌ها دانست بلکه ماهیت آنها به گونه‌ای است که در تمام مراحل حاکمیت داشته و روح حاکم بر مقررات حریم خصوصی می‌باشند. ذیلاً اهم این اصول را در دو بند مورد بررسی قرار می‌دهیم.

۶-۱-اصل رضایت (Consent Principle)

هدف از تدوین مقررات حمایت از داده‌های شخصی در درجه اول صیانت از حقوق شهروندان است. لذا علی‌الاصول در اغلب موارد اخذ رضایت سوژه می‌تواند وصف ممنوعیت و تخلف را از اعمال ناقض حریم خصوصی (در هریک از مراحل تحصیل، پردازش و انتقال و امحاء داده‌ها) سلب نماید. مع‌الوصف ذکر چند نکته ضروری است:

- **نخست** آنکه رضایت سوژه زمانی می‌تواند دارای چنین کارکردی باشد که اطلاعات کافی و روشنگر در خصوص موضوعی که نسبت بدان اخذ اجازه می‌شود به او داده شده باشد.
- **دوم** آنکه سوژه واقعاً مخیر در اعلان یا عدم اعلان رضایت باشد.
- **سوم** آنکه اخذ رضایت حتی‌المقدور پیش از عمل باشد مگر اینکه اجازه را نوعی ابراء متخلف تلقی کنیم.
- **چهارم** آنکه در موارد استثنایی و مصرح بویژه مواردی که با منافع عمومی و امنیت جامعه ارتباط پیدا می‌کند قانون می‌تواند مقرر کند که رضایت سوژه در ممنوع بودن عمل بی تاثیر است[۲۰].

همچنین باید بخاطر داشت که سوژه همیشه باید این حق را داشته باشد که رضایت خود را بازپس گیرد، هرچند این عمل نسبت به اعمالی که پردازشگر قبل از آن انجام داده است بی‌تأثیر است.

۶-۲- اصل مسؤولیت(Redress Principle)

تفاوت مهم قاعده حقوقی با قاعده و توصیه اخلاقی در اینست که اولی واجد ضمانت اجرای مادی و بیرونی است و دومی تنها ضمانت اجرای درونی و وجدانی دارد.[۲۱] احکام قانونگذار اگر فاقد ضمانت اجرا و مسؤولیت برای متخلف باشند ارزش چندانی در نظام حقوقی نداشته و از نیل به مقصود (نظم و عدالت) باز می‌مانند.

در حوزه حقوق فناوری اطلاعات و بویژه بحث حمایت از داده نیز وضع به همین منوال است و صرفنظر از ماهیت مسؤولیت (مدنی یا کیفری یا انتظامی) در هر حال باید متخلف را مسؤول سرپیچی از حکم قانونگذار دانست. البته بدیهی است که اعمال این اصل در هر مورد، بالاخص با توجه به ماهیت مسؤولیت مشروط به تحقق شرایط و عناصر عمومی و اختصاصی مسؤولیت می‌باشد. همچنین از دیگر آثار این اصل ضرورت برخورداری شهروندان از روش‌های تعقیب و دادخواهی مناسب می‌باشد که به عنوان راهکار اجرایی تحقق اصل مسؤولیت ضرورت دارد.

لذا بر اساس این اصل می‌توان گفت که گردآورنده، و پردازشگر داده‌ها نسبت به تخلف از احکام قانونی و تجاوز به حریم خصوصی شهروندان علی‌الاصول و مشروط به تحقق شرایط عمومی و اختصاصی مسؤولیت دارد و شهروندان در هرحال حق دادخواهی و تقاضای بهره‌مندی از روش‌های جبران (Remedies) را دارند.[۲۲]

نتیجه

۱- اصول حاکم بر حمایت از داده‌های کلی حقوقی است که راهنمای قانونگذار در تدوین قوانین و قضات در رسیدگی‌های قضایی می‌باشد.

۲- این اصول به پنج قسم قابل انقسامند:
- اصول مربوط به تحصیل داده‌ها
- اصول مربوط به نگهداری داده‌ها
- اصول مربوط به بکارگیری داده‌ها
- اصول مربوط به امحاء و انتقال داده‌ها
- سایر اصول

۳- اصول مربوط به تحصیل داده‌ها عبارتند از:
- اصل تحصیل قانونی و منصفانه
- اصل تحصیل مضیق و مرتبط
- اصل انتخاب
- اصل اطلاع

۴- اصول مربوط به نگهداری داده‌ها عبارتند:
- اصل امنیت
- اصل شفافیت
- اصل دسترسی
- اصل صحت

۵- اصول مربوط به بکارگیری داده‌ها عبارتند از:

- اصل پردازش مرتبط
- اصل ممنوعیت افشاء

۶- اصول مربوط به امحاء و انتقال داده‌ها عبارتند از:

- اصل امحاء
- اصل عدم انتقال

۷- سایر اصول حاکم بر حمایت از داده عبارتند از:

- اصل رضایت
- اصل مسؤولیت

مراجع:

1 - David Banisar, Privacy&Human Rights, Electrinic Privacy Information Center, 2000,Washington DC,p3
2-http://www.dataprivacy.ie/6aii-2.htm#6
3-http://www2.austlii.edu.au/itlaw/articles/IPPs.html
4- http://profs.lp.findlaw.com/privacy/3b.html#2
5- http://www.bild.net/privacyusa5.htm
6-http://www.privacy.ca.gov/code/fairinfo.htm
7- Denis Kelleher& Karen Murray,IT Law in the European Union,Sweet&Maxwell,1999,London,p240
8-http://www.workplaceinfo.com.au/nocookie/alert/2001/01329.htm
9-http://www.privacy.gov.au/publications/npps01.html#e
10-http://www2.austlii.edu.au/itlaw/articles/IPPs.html#Heading17
12-http://profs.lp.findlaw.com/privacy/3b.html#3
13-http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s14.html
14-http://www2.austlii.edu.au/~graham/CyberLRes/2001/1/#Heading11
15-http://www.privacy.gov.au/publications/npps01.html#c
16-http://www.privacy.gov.au/publications/npps01.html#b
17-http://www.privacy.gov.au/publications/npps01.html#d
18-http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list
19-http://www.privacy.gov.au/publications/npps01.html#i
20-http://www2.austlii.edu.au/itlaw/articles/Heading17
۲۱- کاتوزیان، دکتر ناصر، *مقدمه علم حقوق و مطالعه در نظام حقوقی ایران*، شرکت انتشار با همکاری بهمن برنا، چاپ بیستم،۱۳۷۴،ص۵۵
22-http://www.bild.net/privacyusa5.htm

☑ **عنوان: مطالعه تطبیقی مقررات حاکم بر مبادلات الکترونیکی**

☑ **نویسنده: مصطفی بختیاروند**

(دانشجوی کارشناسی ارشد حقوق خصوصی دانشگاه امام صادق(ع))

چکیده

تجارت الکترونیکی از رشته‌های پیچیده‌ای است که تنظیم روابط اشخاص در آن مستلزم وضع و اجرای قوانین و مقررات کارآمد توسط افرادی است با دانش فنی و حقوقی کافی. در نوشتار حاضر ابتدا به صورت کلی شرایط ضروری جهت انجام مبادلات الکترونیکی ایمن و مطمئن را مورد بررسی قرار داده‌ایم. در بخش دوم به مطالعه مسایل مربوط به مهم‌ترین دسته این مبادلات یعنی قراردادهای الکترونیکی پرداخته و در نهایت بخش سوم را به حل و فصل اختلافات ناشی از انجام مبادلات در محیط مجازی و ادله الکترونیکی اثبات دعوی اختصاص داده‌ایم.

کلید واژه‌ها

تجارت الکترونیکی ـ مبادلات الکترونیکی ـ حمایت از داده‌ها ـ قراردادهای الکترونیکی ـ ادله اثبات الکترونیکی ـ امضای الکترونیکی ـ امضای دیجیتال ـ مراجع گواهی

مقدمه

اهمیت وجود قوانین و مقرراتی که بتوان با آن روابط اشخاص را در زمینه‌های مختلف تنظیم نمود بر کسی پوشیده نیست. تجارت الکترونیکی از زمینه‌هایی است که علیرغم پیشینه کوتاه خود به سرعت متحول شده و روزبروز بر گستردگی و پیچیدگی آن افزوده می‌شود. یکی از مهم‌ترین اصول در تجارت اصل سرعت است و تجارت الکترونیکی وسیله‌ای است جهت تضمین سرعت در اعمال تجاری: امکان بازدید از پایگاه‌های مختلف و آگاهی از کیفیت و نحوه ارایه کالاها و خدمات و سفارش آن با صرف اندک وقت و هزینه موجب شده که این رشته در کشورهای مختلف با استقبال گسترده‌ای مواجه شود. اما آیا فعالیت‌های تجاری در محیط مجازی را همچنان می‌توان به وسیله قوانین مربوط به تجارت سنتی اداره کرد؟ با قدری تأمل در ویژگی این نظام نوین تجاری مسلماً پاسخ ما منفی خواهد بود. مسایل و موضوعات پیچیده‌ای در انجام مبادلات الکترونیکی وجود دارد که بی‌سابقه بوده و پاسخگویی مناسب به آن بدون در دست داشتن قوانین مطلوب ممکن نیست: در فضای مجازی اشخاص بدون نیاز به حضور فیزیکی با هم ارتباط برقرار می‌کنند و چه بسا فردی با هدف سوء استفاده از فرصت فراهم شده هویتی جعلی برای

خود برگزیند و طرف دیگر را که خلع سلاح بوده و هیچ وسیله‌ای برای شناسایی هویت حقیقی و تعقیب وی در دسترس ندارد با مشکلات فراوانی مواجه سازد. همچنین ممکن است اطلاعاتی که اشخاص از طریق شبکه‌ای مانند اینترنت با هم مبادله می‌کنند توسط اشخاص غیر مجاز شنود یا دستکاری شده و این امر زیان‌های جبران‌ناپذیری به آنها وارد سازد، دریافت کننده اطلاعات نیز ممکن است اطلاعات دریافتی را در راهی جز هدف اعلام شده به کار گیرد و یا آنها را در اختیار اشخاص غیر مجاز قرار دهد. پس لازم است در این خصوص چاره‌ای اندیشید و مبادلات الکترونیکی را از امنیت کافی برخوردار نمود. مهمترین نوع مبادلات الکترونیکی، قراردادهای الکترونیکی هستند که علاوه بر شناسایی قانونی، تشخیص زمان و مکان انعقاد این نوع قراردادها از اهمیت ویژه‌ای برخودار است و از جمله در تشخیص قانون حاکم بر روابط طرفین و دادگاه صالح جهت رسیدگی به اختلافات آنان نقشی اساسی ایفا می‌کند. وقوع اختلاف میان اشخاص در جریان انجام فعالیت‌های تجاری امری اجتناب‌ناپذیر است و در این موارد وجود سیستم‌های کارآمد، برای حل و فصل اختلافات در کمترین زمان ممکن از بدیهیات بوده و به تبع آن با این پرسش مواجهیم که آیا اسناد الکترونیکی را می‌توان به عنوان ادله اثبات دعوی به کار برد؟

در این مقاله که حاصل مطالعه تطبیقی مهمترین قوانین و اسناد بین‌المللی و ملی موجود در این زمینه است سعی ما بر آن بوده که مسایل مذکور را بررسی نموده و در خصوص آنها نتایجی قابل قبول ارایه نماییم. این واقعیت را نباید از نظر دور داشت که پرداختن به مباحث مرتبط با حقوق تجارت الکترونیکی در کشور ما سابقه طولانی ندارد و این رشته در مراحل نخستین شکل‌گیری به سر می‌برد و بی‌شک محلی است بسیار مناسب برای اهل تحقیق و مشتاقان فراگیری مسائل نوین حقوقی.

بخش نخست: شرایط لازم جهت انجام مبادلات الکترونیکی[1] ایمن و مطمئن

مهمترین ویژگی مبادلات الکترونیکی مجازی بودن فضایی است که این مبادلات در آن صورت می‌پذیرند. در چنین فضایی احتمال تقلب و سوء استفاده از اعتماد مشروع طرف مقابل توسط سودجویان بسیار بالا بوده و تاکنون نمونه‌های فراوانی از این نوع تخلفات گزارش شده است. به عنوان نمونه در آگوست سال ۲۰۰۲ خبرگزاری رویترز از توقف مبادله سهام به صورت بر خط (on-line) در پی افشای خبر استفاده غیر مجاز فردی از حساب یکی از مشتریان شرکت دوو سکیوریتیز (DAEWOO Securities) چهارمین کارگزار عمده بورس کره جنوبی و خرید سهامی به ارزش ۲۲ میلیون دلار با استفاده از حساب مذکور خبر داد. فرد مورد نظر توانسته بود که در طی ۹۰ ثانیه تعداد ۵ میلیون سهم از سهام شرکت دلتا (Delta) را به خود منتقل کند. انتشار این خبر موجب سلب اعتماد گسترده تجار نسبت به مبادلات برخط (on-line) شده و

---

[1]- اصطلاح مبادله الکترونیکی (Electronic transaction) مفهومی اعم از قرارداد الکترونیکی (Electronic Contract) دارد. قانون یکنواخت مبادلات الکترونیکی ایالات متحده (UETA) در ماده «۲» اصطلاح مبادله الکترونیکی را بدین صورت تعریف کرده است: «عمل یا مجموعه‌ای از اعمال حادث میان دو یا چند شخص در ارتباط با انجام امور مربوط به کسب و کار، تجارت یا امور دولتی» بنابراین ارسال اطلاعات مربوط به زندگی شخصی و کاری فرد (Resume) برای یک شرکت در پی انتشار آگهی استخدام توسط شرکت مذکور مبادله‌ای الکترونیکی است و نه قرارداد.

از زبان یکی از سرمایه‌گذاران بزرگ کره جنوبی نقل شده بود که: «ما از امروز به دلایل امنیتی تجارت الکترونیکی را متوقف می‌نماییم»[۲].

بنابراین تجار و مصرف‌کنندگان باید پیش از به کارگیری سیستم‌های باز[۳] ارتباطی مانند اینترنت نسبت به موضوعات زیر اطمینان حاصل نمایند:[۴]

۱ـ شناسایی هویت واقعی فرستنده پیغام الکترونیکی[۵]: آیا اشخاصی که با آنها ارتباط برقرار نموده و پیغام‌هایی مبادله نموده‌ایم واقعاً همان کسانی هستند که ادعا می‌کنند؟ آیا هویت و مشخصات اعلام شده واقعاً متعلق به خود آنها است؟ همانطور که گفتیم، مجازی بودن محیط تجارت الکترونیکی موجب شده که اشخاص مبادلات خود را از راه دور و بدون مشاهده یکدیگر و یا شنیدن صدای طرف مقابل صورت دهند و درنتیجه، دریافت کننده پیغام الکترونیکی حق دارد نسبت به اصالت هویت فرستنده پیغام با احتیاط بیشتری برخورد کرده، هویت واقعی وی را تشخیص داده و مطمئن شود که پیغام واقعاً از سوی او ارسال شده است. برای نمونه در صورتی که بانک دستور پرداخت وجهی به شخص ثالثی را به صورت الکترونیکی دریافت کند این مؤسسه باید بتواند منبع این دستور را شناسایی کرده، مطمئن شود حقه‌ای در کار نیست و آنگاه مبادرت به پرداخت وجه مورد نظر نماید[۶].

۲ـ تمامیت داده‌ها[۷]: آیا داده‌های تشکیل دهنده پیغام الکترونیکی در جریان انتقال، چه به صورت عمدی و چه غیر عمدی، دستکاری[۸] شده‌اند یا نه؟ آیا می‌توان مطمئن بود که پیغام دریافتی همان پیغامی است که توسط فرستنده ارسال شده یا ثالثی برخی از داده‌های موجود در آن را حذف کرده، تغییر داده و یا مطلبی به آن افزوده است؟ فرض کنیم رستورانی در شهر تهران سفارش تهیه غذا برای ۱۵۰۰ نفر را از سوی یکی از مشتریان خود دریافت می‌کند. در موعد مقرر غذا آماده می‌شود ولی هنگام تحویل مشتری اعلام می‌کند که وی صرفاً برای ۱۵۰ نفر غذا سفارش داده است و مشخص می‌شود که شخص دیگری محتوای پیغام مذکور را تغییر داده است.

۲- http://asia.tech.yahoo.com

۳- open systems که در آنها طرفین از پیش درخصوص حقوق و تکالیف خود توافق نکرده اند و یکدیگر را نمی‌شناسند. در مقابل سیستم‌های بسته (closed systems) که در آنها طرفین مبادله الکترونیکی قبل از ورود به محیط الکترونیکی در خصوص نحوه انجام این مبادلات و حقوق و تکالیف خود توافق می‌کنند و هویت هر یک از طرفین برای طرف دیگر آشکار است. نک.ستار زرکلام، امضای الکترونیکی و جایگاه آن در نظام ادله اثبات دعوی، فصلنامه علمی پژوهشی دانشکده علوم انسانی (حقوق) دانشگاه تربیت مدرس، بهار ۱۳۸۲

۴- www.info.gov.hk

۵- Authenticity

۶- Tomas J. Smedinghoff,The legal requirements for creating secure and enforceable electronic transactions,p.17

۷- Data integrity

۸- Manipulation

۳ـ عدم قابلیت انکار[۹]: دریافت کننده پیغام الکترونیکی زمانی تمایل خواهد داشت که اقداماتی (مانند ارسال کالا، انتقال وجوه و ...) را بر مبنای این پیغام انجام دهد که مطمئن باشد در صورت بروز اختلاف خواهد توانست ثابت کند که طرف مقابل آن را ارسال داشته (هرگاه واقعاً وی پیغام را فرستاده باشد) و نیز مانع ادعای تفاوت محتوای پیغام دریافتی با داده پیام ارسالی توسط فرستنده شود (البته هر گاه واقعاً آنچه دریافت شده دقیقاً همان پیغامی باشد که فرستنده ارسال کرده است). عدم قابلیت انکار در حقیقت نتیجه تشخیص هویت واقعی فرستده و اطمینان نسبت به تمامیت داده‌ها خواهد بود.

٤ـ حفظ محرمانگی[۱۰]: آیا داده‌های موجود در پیغام الکترونیکی مخفی نگه داشته شده و منحصراً فرستنده و دریافت کننده مورد نظر قادر به خواندن و فهم آن خواهند بود؟ در دنیای امروز اطلاعات اهمیت ویژه‌ای دارند: گاه حفظ مزیت رقابتی یک مؤسسه تجاری مستلزم آن است که اطلاعات معینی همیشه جنبه محرمانه داشته باشند، برخورداری از اطلاعات کافی در خصوص مشتریان و حفظ این اطلاعات لازمه بازاریابی موفق است، برخی اطلاعات نیز جنبه مالی نداشته و در جریان ارتباطات الکترونیکی دوستانه منتقل می‌شود مثلاً شماره شناسنامه، سن اشخاص، مشکلات روحی و .... حال اگر طرفین مبادله الکترونیکی نسبت به حفظ این اطلاعات اطمینان حاصل ننمایند نمی‌توان شاهد گسترش تجارت و ارتباطات الکترونیکی بود.

در واکنش به این دغدغه‌ها و جهت شناسایی امضاء کننده، تضمین تمامیت داده‌ها، جلوگیری از انکار انتساب و محتوای پیغام الکترونیکی و نیز حفظ محرمانگی اطلاعات، انواع امضاهای الکترونیکی به وجود آمده‌اند که اشخاص می‌توانند در انجام مبادلات الکترونیکی از آنها استفاده نمایند. این موضوع در بخش سوم مورد بررسی قرار خواهد گرفت.

– حمایت از داده ها[۱۱]

اما مناسب است که در این مجال به مسأله حمایت از داده‌ها نیز بپردازیم. از لوازم اولیه انجام مبادلات الکترونیکی به طریقی مطمئن و تشویق اشخاص به تجارت الکترونیکی وضع قوانین مطلوب در زمینه حفظ حریم خصوصی[۱۲] اعضای جامعه است زیرا حق حفظ حریم خصوصی از بدیهی‌ترین حقوق افراد است و به علاوه همانطور که اشاره شد، اطلاعات در دنیای امروز ارزشی بیش از گذشته دارند، برخی اطلاعات نیز از حساسیت ویژه‌ای برخوردار هستند[۱۳] که حفظ آنها را ایجاب می‌کند مانند اطلاعاتی که بیمار یا موکل به پزشک یا وکیل خود ارایه می‌دهند، عقاید سیاسی و .... در این خصوص دستورالعمل ۹۵/۴۶/EC پارلمان و شورای اروپا پنج اصل را مقرر داشته و کشورهای عضو را ملزم نموده تضمین کنند که داده‌های شخصی:

الف) به صورت منصفانه و قانونی پردازش می‌شوند؛

ب) برای اهداف معین، صریح و قانونی جمع‌آوری شده و بعداً به روشی مغایر با اهداف مذکور پردازش نخواهند شد؛

۹ـ Non-repudiation

۱۰ـ Confidentiality

۱۱ـ Data Protection

۱۲ـ Privacy

۱۳ـ Sensitive data

ج) با اهداف جمع‌آوری یا پردازش متناسب و مرتبط بوده و فراتر از آن نباشند؛

د) صحیح و دقیق بوده و در موارد ضروری به صورت روزآمد نگهداری می‌شوند؛ تمامی اقدامات معقول و متعارف باید جهت تضمین این امر صورت گیرد که داده‌های ناصحیح یا غیر متناسب با اهداف جمع‌آوری یا پردازش بعدی داده‌ها، حذف یا تصحیح می‌شوند؛ و

ه) به صورتی نگهداری می‌شوند که شناسایی اشخاص موضوع داده‌ها را برای مدت زمان ضروری جهت نیل به اهداف جمع‌آوری یا پردازش بعدی آنها ممکن می‌سازد[۱۴].

تجار باید رویه‌های خود در خصوص جمع‌آوری و انتشار اطلاعات را به آگاهی اشخاص موضوع اطلاعات برسانند و به اصطلاح «سیاست حفظ حریم خصوصی[۱۵]» مراجعه‌کنندگان را اعلام نمایند. به عنوان مثال تجار باید مشخص کنند که:

الف) چه نوع اطلاعاتی از مراجعه‌کنندگان جمع‌آوری می‌شود.

ب) نحوه به کارگیری اطلاعات چگونه خواهد بود.

ج) چه کسی از اطلاعات آگاه خواهد شد.

د) آیا اشخاص موضوع اطلاعات حق خواهند داشت مانع استفاده از آنها یا مطلع شدن اشخاص ثالث شوند.

ه) آیا اطلاعات بعداً روزآمد خواهد شد.

و) آیا تقاضای حذف اطلاعات از پایگاه داده تاجر پذیرفته خواهد شد.

این سیاست باید طی اعلامیه‌ای به اطلاع مراجعه‌کنندگان برسد و در صورت تحقق شرایط، گواهی مبنی بر مطلوبیت سیاست حفظ حریم خصوصی از سوی مرجع مربوط صادر خواهد شد. این مرجع می‌تواند عملکرد تاجر در خصوص حفظ حریم خصوصی بازدیدکنندگان از پایگاه (وب سایت) وی را گهگاه مورد ارزیابی قرار داده و در صورت عدم اجرای سیاست اعلامی ضمانت اجرای پیش‌بینی شده (از قبیل جریمه، الغای گواهی مطلوبیت و ...) را علیه او اعمال نماید[۱۶].

مواد ۶۲ تا ۶۵ قانون تجارت الکترونیکی جمهوری اسلامی ایران به «حمایت از داده پیام‌های شخصی» اختصاص یافته است. ماده ۶۲ قانون مذکور مقرر می‌دارد: «دریافت، ذخیره، پردازش و یا توزیع داده پیام‌های شخصی مبین ریشه‌های قومی یا نژادی، دیدگاه‌های سیاسی، عقیدتی، مذهبی، اعتقادات فلسفی و اخلاقی، عضویت در اتحادیه‌های صنفی و احزاب و داده پیام‌های راجع به وضعیت جسمانی، روانی و یا زندگی جنسی اشخاص بدون رضایت صریح آنها به هر عنوان غیر قانونی است». در ماده ۶۳ نیز اصولی مشابه اصول دستورالعمل (فوق‌الذکر) اتحادیه اروپا مقرر شده و در ماده ۶۴ داده پیام‌های مربوط به سوابق پزشکی و بهداشتی تابع مقررات ویژه دانسته شده است. در ماده ۶۵ از جمله، موضوع نهادهای مسؤول دیده‌بانی و کنترل جریان داده پیام‌های شخصی و تشکیلات و وظایف آنها به تصویب قانون خاص و آیین‌نامه موکول شده است.

در مواد ۷۷ تا ۸۵ نیز مجازات‌هایی برای نقض حریم خصوصی و داده‌های مربوط به اشخاص پیش‌بینی شده است.

۱۴- WWW. bka.gv

۱۵- Privacy Policy

۱۶- Christine Hart,Online dispute resolution in electronic commerce, PP. 6-7

بخش دوم: قراردادهای الکترونیکی

۱ـ شناسایی قانونی قراردادهای الکترونیکی

در ابتدای بحث بهتر است به این پرسش بپردازیم که آیا ارسال پیغام‌های الکترونیکی و یا به صورت خیلی ساده‌تر کلیک کردن بر روی عبارتی خاص را می‌توان به عنوان شیوه معتبری برای اعلام اراده و تحقق ایجاب و قبول تلقی نمود یا خیر؟ ساده‌ترین و در عین حال متداول‌ترین وسیله تفاهم معانی الفاظ است. مرسوم است که دو طرف عقد برای تعیین شرایط معامله به گفتگو بپردازند و پس از توافق نیز اراده خود را به هم بگویند. اگر اینان در یک محل و در حضور هم نباشند این مذاکره و توافق با تلفن و رادیو نیز ممکن است.

اعلام اراده به وسیله نوشته نیز در حکم بیان الفاظ است. زیرا نوشته نیز مانند صوت وسیله عرفی و عادی انتقال معانی است و از این جهت تفاوتی بین وجود لفظی و کتبی کلمه‌ها وجود ندارد. پس طرفین می‌توانند به وسیله تلگرام یا نامه خصوصی یا اعلان در روزنامه با هم معامله کنند. نباید چنین پنداشت که لفظ تنها وسیله بیان صریح اراده است. زیرا چه بسا اشاره‌ای که بلیغ‌تر از هزاران کلمه است. وانگهی در پاره‌ای معامله‌ها، مانند حراجها و مزایده‌ها، اشاره وسیله متعارف بیان اراده و شایع‌تر از سخن گفتن است. الفاظ به خودی خود، در انعقاد قراردادها اثری ندارد و تنها وسیله تبادل افکار و خواست‌های طرفین است. پس هر وسیله دیگری که بتواند این وظیفه را انجام دهد ممکن است در بیان اراده به کار رود. در ماده ۱۹۱ قانون مدنی هر چیز که دلالت بر مقصود انشاء کننده نماید، برای تحقق عقد کافی دانسته شده است.[۱۷] بنابراین از آنجا که در عرف، ارسال پیغام‌های الکترونیکی و یا کلیک کردن بر روی عبارتی خاص دال بر قصد انشای طرفی است که این اعمال را انجام می‌دهد و در قانون مدنی اعلام اراده به وسیله خاصی مقید نشده است پاسخ به سؤال فوق‌الذکر مثبت خواهد بود و این پاسخ مقدمه‌ای است برای پذیرش اعتبار قراردادهای الکترونیکی، حتی اگر قانون خاصی در رابطه با این قراردادها در کشور ما وجود نداشته باشد.

اما نظر به اهمیت قراردادهای الکترونیکی و نقش آن در توسعه اقتصادی کشورها و کاهش هزینه‌ها و افزایش سرعت فعالیت‌های تجاری، قانونگذاران در سطح ملی و بین‌المللی به‌طور خاص و صریحاً به اعتبار قراردادهای الکترونیکی اشاره کرده‌اند. به عنوان مثال، قانون نمونه تجارت الکترونیکی کمیسیون سازمان ملل متحد برای حقوق تجارت بین الملل با نام اختصاری آنسیترال[۱۸] در ماده۱۱ (۱) مقرر می‌دارد: «جز در صورت وجود توافق دیگر میان طرفین، جهت انعقاد قرارداد، ایجاب و قبول آن را می‌توان از طریق داده پیام صورت داد. هرگاه داده پیامی در جریان انعقاد یک قرارداد به کار رود، اعتبار یا قابلیت اجرای قرارداد مذکور را نمی‌توان صرفاً به دلیل استفاده از داده پیام به این منظور [انعقاد قرارداد] رد کرد».

قانون یکنواخت مبادلات الکترونیکی آمریکا (UETA) نیز در ماده۷ (ب) مقرر داشته: «اثر قانونی یا قابلیت اجرای قرارداد را صرفاً به دلیل استفاده از یک رکورد (سند) الکترونیکی در انعقاد آن نمی‌توان ردّ کرد».

---

[۱۷]– دکتر ناصر کاتوزیان، قواعد عمومی قراردادها، ج اول، صص ۲۵۸ ـ ۲۵۷

[۱۸]– En: UNCITRAL,Fr: CNUDCI

در قانون تجارت الکترونیکی جمهوری اسلامی ایران ماده صریحی در این خصوص مشاهده نمی‌شود ولی می‌توان از ماده ۱۲ این قانون که بیان می‌دارد: «اسناد و ادله اثبات دعوی ممکن است به صورت داده پیام بوده و داده پیام در مقام دعوی یا دفاع معتبر است. در هیچ محکمه یا اداره دولتی نمی‌توان براساس قواعد ادله موجود، ارزش اثباتی داده پیام را صرفاً به دلیل شکل و قالب آن ردّ کرد»، اعتبار قراردادهای الکترونیکی را استنباط نمود. زیرا مسلماً از مواردی که طرفین به ادله الکترونیکی استناد می‌کنند هنگامی است که در خصوص قراردادی که به صورت الکترونیکی و با استفاده از داده پیام منعقد نموده‌اند دچار اختلاف می‌شوند، که در این صورت مجاز دانستن استناد به پیغام‌های الکترونیکی به کار رفته در انعقاد این قرارداد به معنی معتبر شناختن اعلام اراده از طریق داده پیام است.

۲ـ زمان و مکان انعقاد قراردادهای الکترونیکی

قـــرارداد الکترونیکی در چه زمان و مکانی منعقد شده محسوب می‌شود؟ مسلماً قرارداد هنگامی تشکیـــل می شود که قبول به ایجاب منضم شود اما مسأله اصلی این است که قبول در چه زمانی محقق می‌شود؟ پاسخ به این پرسش از جمله در جهت تعیین قانون حاکم بر روابط طرفین قرارداد و تشخیص دادگاه صالح در رسیدگی به اختلافات آنها از اهمیت خاصی برخوردار است[۱۹]. همچنین در مواردی که بین افراد در قبول مفاد ایجاب رقابت وجود داشته باشد (مانند حالتی که کالای خاصی به کسی فروخته می‌شود که زودتر قبولی خود را اعلام کرده باشد) یا در صورتی که ایجاب کننده از ایجاب رجوع نماید، تعیین زمان قبول نقش مهمی ایفا خواهد نمود. از آنجا که سابقاً طرفین قرارداد در یک کشور بوده و بیشتر قراردادها به صورت حضوری منعقد می‌شد، در خصوص زمان و مکان تشکیل قرارداد در یک کشور بوده و بیشتر قراردادها به صورت حضوری منعقد می‌شد، در خصوص زمان و مکان تشکیل قرارداد مشکل خاصی به وجود نمی‌آمد، اما به تدریج که استفاده از وسایل ارتباطی مانند نامه، فکس، تلکس و (به ویژه در سال‌های اخیر) پست الکترونیکی و ... جهت انجام مبادلات بین‌المللی (اعم از تجاری و ...) گسترش یافت مسأله تعیین زمان و مکان انعقاد قرار داد به شکل جدی‌تری مطرح گردید[۲۰].

اکنون جهت یافتن پاسخی مناسب برای پرسش مطرح شده، میان دو دسته از قراردادهای الکترونیکی تفکیک مینمائیم:

الف) قراردادهای منعقده از طریق وب سایت[۲۱]

تعیین زمان تحقق قبول، در قراردادهایی که بر روی وب جهانی منعقد می‌شوند مشکل ویژه‌ای را مطرح نمی‌کند، زیرا وب جهانی از خصوصیات یک ارتباط فوری و همزمان برخوردار است. پس این نوع قراردادها را می‌توان در حکم قراردادهایی دانست که در آن طرفین حضور فیزیکی دارند و بنابراین هنگامی که مخاطب ایجاب قبولی خود را (مثلاً از طریق کلیک کردن بر روی عباراتی مانند موافقم و ...) اعلام می کند قرارداد منعقده شده محسوب می‌شود. مکان انعقاد قرارداد نیز مکان استقرار قبول کننده خواهد بود.

ب) قراردادهای منعقده از طریق پست الکترونیکی[۲۲]

۱۹- دکتر ناصر کاتوزیان، قواعد عمومی قراردادها، ج اول، صص ۳۷۶-۳۷۴

۲۰- Michael Chissick,Alistair Kelman, Electronic Commerce,Law and Practice,p.79

۲۱- Website contracts

پست الکترونیکی به عنوان معادل الکترونیکی پست سنتی محسوب می‌شود. ارتباط از طریق پست الکترونیکی به طور معمول ارتباطی فوری و همزمان محسوب نمی‌شود. بنابراین می‌توان قراردادهای منعقده از این طریق را به عقود مکاتبه‌ای ملحق نموده و احکام عقود اخیرالذکر را در خصوص آنها اعمال نمود.[۲۳] در خصوص عقود مکاتبه‌ای چهار نظریه ارایه شده و تعیین زمان و مکان تشکیل قرارداد بسته به این است که قایل به کدام نظریه باشیم. این نظریات عبارتند از: اعلام قبول، ارسال قبول، وصول قبول و اطلاع از قبول[۲۴].

ارسال قبول حاکی از انشاء قبول در ذهن و وسیله‌ای است برای اعلام اراده[۲۵] و با توجه به ماده ۱۹۱ قانون مدنی که می‌گوید: «عقد محقق می‌شود به قصد انشا به شرط مقرون بودن به چیزی که دلالت بر قصد کند» وصول قبول یا اطلاع موجب از آن ضروری دانسته نشده است. بنابراین در سیستم حقوقی ایران نظریه ارسال قابل دفاع و با مقررات و قواعد و اصول حقوقی این سیستم منطبق می‌باشد.[۲۶] البته برخی از علمای حقوق، به حق، معتقدند که هرگاه پیش از ارسال، حصول قبول با استناد به دلیلی احراز شود، این زمان ملاک خواهد بود.[۲۷]

حال با این پرسش مواجهیم که ارسال پیغام الکترونیکی در چه زمانی صورت می‌گیرد؟ ماده ۱۵ قانون نمونه آنسیترال تحت عنوان زمان و مکان ارسال و دریافت داده پیام‌ها مقرراتی در این خصوص پیش‌بینی نموده است. برای نمونه در پاراگراف (۱) این ماده آمده است: «در صورت عدم توافق دیگر میان اصل‌ساز و مخاطب، ارسال داده پیام زمانی صورت می‌گیرد که داده پیام به سیستم اطلاعاتی خارج از کنترل اصل‌ساز یا شخصی که به نمایندگی از وی آن را ارسال کرده وارد شود». پس هنگامی که پیغام الکترونیکی دالّ بر قبول به سیستم اطلاعاتی وارد شود که خارج از کنترل قبول کننده قرار دارد، عقد منعقد شده محسوب می‌شود و مکان انعقاد عقد هم مکان استقرار سیستم مذکور خواهد بود. در قانون تجارت الکترونیکی جمهوری اسلامی ایران (مواد ۳۴ـ۳۰) و قانون یکنواخت مبادلات الکترونیکی آمریکا (در ماده ۱۵) نیز مقررات مشابهی پیش‌بینی شده است.

لازم به ذکر است که زمان و مکان ارسال (و دریافت) داده پیام‌ها علاوه بر تشکیل قراردادها، در زمینه‌های دیگری نیزحائز اهمیت است: برای نمونه هرگاه برای تقدیم مدرکی (از قبیل تقاضانامه و ...) به یک اداره دولتی، دادگاه و ... مهلت خاصی تعیین شده باشد تشخیص تقدیم به موقع یا عدم تقدیم به موقع این مدرک با توجه به مقررات فوق‌الذکر ممکن خواهد بود. بدیهی است که با تحقق شرایط مذکور در این مقررات حتی اگر هیچ فردی از ورود داده پیام به سیستم مورد نظر مطلع نباشد نیز داده پیام دریافت شده فرض می‌شود[۲۸].

۲۲- E-mail contracts

۲۳- Michael chissick, Alistair Kelman, ibid, pp. 80-82

۲۴- دکتر مهدی شهیدی، تشکیل قراردادها و تعهدات، ص۱۶۱

۲۵- دکتر ناصر کاتوزیان، همان، ص ۳۶۱

۲۶- دکتر مهدی شهیدی، همان، ص ۱۶۲

۲۷- دکتر سید حسین صفائی، جزوه درسی حقوق مدنی ۹، دانشگاه امام صادق (ع)

۲۸- Tomas J. Smedinghoff, ibid

۳ـ خیار مجلس در قراردادهای الکترونیکی

آیاخیار مجلس در قراردادهای الکترونیکی قابل اعمال هست یا نه؟ می‌دانیم که مدرک خیار مجلس حدیث نبوی «البیّعان بالخیار ما لم یفترقا» است. با توجه به اینکه اصل بر لزوم قراردادها است بنابراین وجود چنین خیاری استثنایی بر این اصل بوده و باید به قدر متیقن آن اکتفا نمود. قدر متیقن این استثنا هم جایی است که طرفین در یک مجلس بوده و حضور فیزیکی داشته باشند و عقد بیع را منعقد نمایند. حال جهت پاسخ به پرسش مطرح شده میان دو دسته از قراردادهای بیع الکترونیکی تفکیک می‌نماییم: ابتدا به قراردادهایی اشاره می‌کنیم که در آنها قبول بلافاصله به ایجاب منضم نمی‌شود مثلاً قبول چند روز بعد از دریافت ایجاب ارسال می‌شود. در این موارد از آنجا که وجود مجلس عقد قابل تصور نیست، نمی‌توانیم قایل به وجود خیار مجلس شویم. اما تردید در خصوص قراردادهایی بیشتر است که در آنها قبول بلافاصله ارسال می‌شود. مثلاً شخصی به پایگاه (سایت) یک تاجر مراجعه کرده و پس از انجام مذاکرات قبولی خود در خصوص خرید کالای مورد نظر را به طرف مقابل اعلام می‌کند. در این حالت ممکن است گفته شود که طرفین اگرچه حضور فیزیکی ندارند ولی ارتباط فکری و روانی آنها برقرار است، پس باید قایل به وجود خیار مجلس برای طرفین باشیم، ولی همانطور که گفتیم اصل بر لزوم قراردادها و پایبندی به پیمان منعقد شده است و خیار مجلس استثنایی است بر این اصل و در مورد استثناء باید به قدر متیقن و آنچه مورد توافق است و در خصوص آن تردید نداریم اکتفا کرد. در حالتی که طرفین در یک مجلس حضور دارند هیچ کس نسبت به وجود خیار مجلس تردیدی به خود راه نمی‌دهد ولی در حالات و موارد دیگر همینکه در خصوص وجود یا عدم خیار مجلس مردد شدیم باید به اصل لزوم مراجعه کرده و قایل به عدم وجود خیار مجلس در این قراردادها شویم[۲۹]، قراردادهای الکترونیکی منعقده میان انسان‌ها از این نوع قراردادها هستند و بنابراین خیار مجلس در آنها قابل اعمال نیست. بدیهی است که انعقاد قرارداد میان انسان و رایانه که طی آن یک طرف مبادله رایانه است و عملیات ویژه صدور ایجاب و قبول را به صورت خودکار و بدون دخالت انسان انجام می‌دهد نیز از قدر متیقن این استثنا خارج بوده و لذا اصل لزوم در این قراردادها نیز جاری خواهد بود.

بخش سوم ـ حل و فصل اختلافات و ادله الکترونیکی اثبات دعوی

۱ـ حل و فصل اختلافات در خارج از دادگاه

بی‌شک در اختلافات مرتبط با تجارت الکترونیکی که موضوع آنها معمولاً مبالغ نسبتاً کمی است توسل به دادگاه‌ها اغلب برای بیشتر مصرف‌کنندگان و تجار کوچک راه‌حلی مفید نیست، بنابراین توصیه می‌شود که استفاده از سازوکارهایی تشویق شود که راه‌حلی سریع و کم‌هزینه را که به راحتی قابل دسترس است برای اختلافات ناشی از شمار بسیاری از معاملات با حجم پایین (یعنی اختلافاتی که ممکن است از معاملات منعقده میان تجار و مصرف‌کنندگان ناشی شود) ارایه می‌دهد. لذا جهت تأسیس یک نظام کارآمد تجارت الکترونیکی باید ساز و کارهای جایگزین[۳۰] (مانند داوری و ...) را در کنار امکان توسل به سیستم قضایی مجاز شمرده و اشخاص را به اتخاذ این راه‌حل‌ها تشویق نماییم[۳۱]. منظور از سازو کارهای جایگزین، راه حل‌های متنوعی است که جهت رسیدگی به دعاوی و حل و فصل اختلافات در خارج از دادگاه اتخاذ می‌شود. این ساز و کارها را متناسب

---

[۲۹]– دکتر ناصر کاتوزیان، عقود معین، ج ۱، ص ۴۸، حجت‌الاسلام دکتر سیدمصطفی مصطفوی، جزوه درسی فقه (۳) دانشگاه امام صادق (ع)

[۳۰]– ADR

[۳۱]– مصطفی بختیاروند (مترجم)، چارچوب تجارت الکترونیکی، خبرنامه انفورماتیک شماره ۸۷، صص ۵۹ـ۵۸

با نقش شخص ثالثی که نفعی در دعوا ندارد می‌توان به دسته‌های مختلفی طبقه‌بندی نمود که دو مورد از آنها عبارتند از میانجی‌گری[۳۲] و داوری[۳۳]. در شیوه نخست صلاحیت تصمیم‌گیری همچنان در اختیار طرفین است و شخص ثالث (میانجی[۳۴]) صرفاً طرفین را در جهت حل و فصل اختلافاتشان مساعدت می‌کند در حالی که در داوری طرفین صلاحیت تصمیم‌گیری و صدور رأی الزام‌آور را به شخص ثالث (داور[۳۵]) اعطا نموده‌اند[۳۶].

دستورالعمل تجارت الکترونیکی اتحادیه اروپا در ماده ۱۷ با عنوان حل و فصل [اختلافات در] خارج از دادگاه، کشورهای عضو را ملزم می‌کند تضمین نمایند که قوانین داخلی آنها مانع به‌کارگیری شیوه‌های حل و فصل اختلافات در خارج از دادگاه نیست.

اشاره به این نکته نیز ضروری است که لزومی ندارد تأسیس سازوکارهای جایگزین نتیجه طرح‌های دولتی باشد، بلکه بخش خصوصی، سازمان‌های غیر دولتی و دیگر اشخاص می‌توانند این برنامه‌ها را ایجاد و آنها را به نحو مؤثری اداره کنند. با وجود این، دولت باید برای توسعه و تشویق این ساز و کارها با دیگر طرف‌های ذینفع همکاری کند.[۳۷]

۲ـ ادله (اسناد) الکترونیکی

در این قسمت ابتدا اهمیت ادله (اسناد) الکترونیکی را بیان نموده و سپس شرایط اعتبار این ادله را با توجه به سیستم‌های مختلف حقوقی بررسی می‌نماییم.

الف) اهمیت ادله (اسناد) الکترونیکی: با گسترش تجارت ا لکترونیکی حجم وسیعی از مبادلات میان تجار به صورت الکترونیکی انجام شده و استفاده از کاغذ در انعقاد قراردادها رونق خود را از دست خواهد داد. پیشتر هم به این نکته اشاره کردیم که تجارت الکترونیکی به دلیل تسهیل فعالیت‌های تجاری، تضمین اصل سرعت در اعمال تجاری و کاستن از هزینه انجام این اعمال مورد توجه تجار قرار گرفته است.درنتیجه اطلاعات مهمی که می‌تواند در رسیدگی به اختلافات و حل و فصل دعاوی مفید واقع شود در سیستم رایانه‌ای و یا به صورتی نگهداری می‌شود که صرفاً توسط رایانه قابل خواندن است. حجم قابل توجهی از اطلاعات ذخیره شده در رایانه نیز هرگز بر روی کاغذ چاپ نمی‌شود[۳۸]. این واقعیت ما را با پرسش مهمی مواجه می‌سازد: آیا اسناد الکترونیکی را می‌توان به عنوان دلیل در دادگاه ارایه نمود؟ با اندکی تأمّل در واقعیت مذکور بی‌تردید پاسخ ما مثبت خواهد بود زیرا عدم پذیرش و شناسایی ادله الکترونیکی نتیجه‌ای جز بلاتکلیفی قرارداد و عدم حلّ و فصل اختلافات و نهایتاً بی‌رغبتی تجار به انجام مبادلات الکترونیکی نخواهد داشت و اصولاً پذیرش اعتبار قراردادهای الکترونیکی

۳۲- Meditation

۳۳- Arbitration

۳۴- Meditator

۳۵- Arbitrator

۳۶- Christine Hart,ibid

۳۷- مصطفی بختیاروند، همان

۳۸- Alan Gahtan, E. evidence law P.1

فرع بر شناسایی قانونی اسناد الکترونیکی است. لذا در قوانین مختلف اعتبار و ارزش اثباتی پیغام‌های الکترونیکی مورد پذیرش قرار گرفته است. به عنوان نمونه کمیسیون سازمان ملل برای حقوق تجارت بین الملل از سال ۱۹۸۶ تلاش برای شناسایی قانونی «دلیل الکترونیکی[۳۹]» را آغاز کرده[۴۰] و سرانجام در سال ۱۹۹۶ با تصویب قانون نمونه تجارت الکترونیکی، از جمله، اعتبار و ارزش اثباتی[۴۱] داده پیام‌ها را پذیرفته است.

ماده ۹ این قانون تحت عنوان پذیرش و ارزش اثباتی داده پیام‌ها مقرر می‌دارد:

« ۱) در رسیدگی‌های قانونی، هیچ یک از مقررات ادله اثبات به گونه‌ای اعمال نخواهد شد که محکمه پسندی داده پیام به عنوان دلیل را صرفاً به علل زیر ردّ نماید:

الف) به دلیل داده پیام بودن آن؛ یا ب) هرگاه داده پیام بهترین دلیل بوده که شخص اقامه کننده آن به طور معقول و متعارف می‌توانسته به دست آورد، به این دلیل که به شکل اصلی خود نیست.

۲) اطلاعات [ارایه شده] به صورت داده پیام از ارزش اثباتی مناسب برخوردار خواهد بود ...».

بند (الف) ماده ۷ قانون یکنواخت مبادلات الکترونیکی آمریکا (UETA) نیز در این زمینه اشعار می‌دارد: «اثر قانونی یا قابلیت اجرای سند یا امضاء را صرفاً به دلیل شکل الکترونیکی آن نمی‌توان رد کرد». همچنین ماده ۱۳ این قانون تحت عنوان «پذیرش [اسناد و امضاهای الکترونیکی] به عنوان دلیل» مقرر نموده: «در جریان رسیدگی به دعاوی، اعتبار سند یا امضاء به عنوان دلیل را صرفاً به دلیل شکل الکترونیکی آن نمی‌توان ردّ کرد.»

در فرانسه قانون ۱۳ مارس ۲۰۰۰ در خصوص هماهنگ‌سازی حقوق ادله اثبات با فناوری‌های نوین و مرتبط با امضای الکترونیکی قانون مدنی این کشور را به صورتی اصلاح نموده که اسناد الکترونیکی نیز به عنوان دلیل پذیرفته شوند. تا پیش از تصویب قانون مذکور با توجه به غلبه اسناد کاغذی، قواعد ادله اثبات مندرج در قانون مدنی به گونه‌ای تفسیر می‌شد که امکان پذیرش اسناد الکترونیکی به عنوان اسناد عادی[۴۲] وجود نداشت[۴۳]. ماده ۱۳۱۶ (جدید) قانون مدنی فرانسه بیان می‌دارد: «دلیل کتبی، صرف نظر از قالب یا روش انتقال آن از مجموعه‌ای از حروف، نشانه‌ها، ارقام و یا هر علامت یا نماد دیگر قابل فهم تشکیل می‌گردد».

(همانطور که قبلاً اشاره شد) ماده ۱۲ قانون تجارت الکترونیکی جمهوری اسلامی ایران نیز داده پیام را به عنوان دلیل و دارای ارزش اثباتی اعلام نموده است.

اما اکنون باید به این پرسش پاسخ دهیم که شرایط شناسایی و پذیرش ادله الکترونیکی کدامند؟ آیا هر سند و مدرک الکترونیکی را می‌توان به عنوان دلیل در دادگاه ارایه کرد؟

۳۹- Electronic Evidence (Proof)

۴۰- Sofian Azzabi, Le nouveau régime probatoire francais … , P.1

۴۱- Evidentiary value

۴۲- les actes sous seing privé در مقابل اسناد رسمی (les actes authentiques)

۴۳- Sofian Azzabi, ibid

ب) شرایط اعتبار ادله (اسناد) الکترونیکی

به‌طور کلی پذیرفتن این اسناد به عنوان دلیل منوط به ایجاد قناعت وجدان در قاضی رسیدگی کننده به دعاوی مطروحه است. با عنایت به ویژگی فضای رایانه‌ای که امکان دستکاری، تغییر، نسخه‌برداری و حذف اطلاعات الکترونیکی را به راحتی فراهم می‌کند، طبیعی است که دادرس در خصوص اعتبار اسناد مذکور با احتیاط بسیار رفتار کرده و در حالت عادی، حداکثر آنها را به عنوان قرینه‌ای بر مدعا تلقی کند. ماده ۲ـ۱۳۱۶ قانون مدنی فرانسه پذیرش ارزش اثباتی معادل اسناد کاغذی برای اسناد الکترونیکی را به تحقق دو شرط منوط نموده است: ۱ـ شخصی که سند از [عمل] او ناشی شده به صورت مطلوبی قابل شناسایی باشد؛ ۲ـ سند الکترونیکی تحت شرایطی تولید و نگهداری شود که تمامیت آن را تضمین نماید.

ماده ۱۳ قانون تجارت الکترونیکی جمهوری اسلامی ایران در این خصوص مقرر می‌دارد: «به‌طور کلی، ارزش اثباتی داده پیام‌ها با توجه به عوامل مطمئنه از جمله تناسب روش‌های ایمنی به کار گرفته شده با موضوع و منظور مبادله داده پیام تعیین می‌شود».

پاراگراف دوم از ماده ۹ قانون نمونه آنسیترال معیارهایی را جهت تعیین ارزش اثباتی داده پیام ارایه نموده نموده است: «میزان اعتبار روش تولید، ذخیره و یا مبادله داده پیام، روش حفاظت از تمامیت داده، روش شناساندن اصل ساز داده پیام و هر عامل مرتبط دیگر».

بدیهی است که با توجه به مقررات فوق‌الذکر گاه ممکن است داده پیام از هیچ ارزش اثباتی برخوردار نباشد (و درنتیجه دلیلی معتبر تلقی نگردد).

ممکن است کسانی با استناد به ماده ۱۲۸۴ قانون مدنی که می‌گوید: «سند عبارت است از هر نوشته که در مقام دعوی یا دفاع قابل استناد باشد»، با پذیرش پیغام‌های الکترونیکی به عنوان سند مخالف نمایند زیرا در این ماده نوشته بودن از شرایط اصلی سند، معرفی شده در حالی که پیغام‌های الکترونیکی نوشته نیستند و نوشته حتماً باید از ثبت جوهر یا ... بر روی کاغذ و ... به وجود آید. این مسأله در گذشته در فرانسه هم مطرح بوده و (همانطور که گفتیم) تا پیش از تصویب قانون ۱۳ مارس ۲۰۰۰ و اصلاح قانون مدنی، به دلیل غلبه نوشته‌های کاغذی، نسبت به پذیرش اسناد الکترونیکی به عنوان ادله کتبی تردید وجود داشت. با اینحال رویه قضایی در این کشور پیش از تصویب قانون مذکور، ادله الکترونیکی را منوط به تحقق شرایطی به رسمیت شناخته و برای آنها همان قدرت اثباتی اسناد عادی را قایل شده بود: دیوان تمیز فرانسه در رأی صادره در تاریخ دوم دسامبر ۱۹۹۷ بیان داشته بود که نوشته ممکن است بر روی هر حاملی (واسط یا قالبی) از جمله از طریق تله‌کپی، ایجاد و نگهداری شود مشروط بر آنکه تمامیت و انتساب آن به نویسندهٔ مشخص شده در نوشته تأیید شده و یا مورد اعتراض واقع نشود[۴۴]».

ب-۱)- نظریه معادل های کارکردی[۴۵]

رأی فوق‌الذکر و به تبع آن، اقدام قانونگذار فرانسوی در اصلاح قانون مدنی این کشور تحت تأثیر نظریه نوینی است با عنوان نظریه «معادل های کارکردی». این نظریه نوشته را به شکل و قالب خاصی محدود نمی‌کند بلکه در عوض کارکردهای

۴۴- Cass. Com.2 Dec.1997

۴۵- The Functional Equivalents

اساسی نوشته را بیان می‌کند و هر مدرکی را که این کارکردها را ارایه دهد به عنوان نوشته تلقی می‌نماید. با توجه به آثار منتشر شده از سوی آنسیترال (که تأثیر قابل توجهی بر شکل‌گیری و رواج این نظریه داشته) می‌توان کارکردهای اساسی نوشته را بدین صورت خلاصه کرد: عدم قابلیت تغییر[۴۶]، قابلیت خوانده شدن[۴۷] و ثبات و دوام[۴۸]. قانونگذار فرانسه و دیوان تمیز این کشور کارکرد «شناسایی[۴۹] شخص منشاء نوشته» و یا به عبارت دیگر «قابلیت انتساب[۵۰] نوشته به شخص معین شده در آن» را نیز به مجموعه مذکور افزوده‌اند[۵۱].

ب-۱-۱)- کارکردهای نوشته

۱- عدم قابلیت تغییر: نوشته باید به صورتی باشد که طرفین یا اشخاص ثالث نتوانند در آن تغییری ایجاد کنند. امکان تغییر دادن آنچه بر روی کاغذ نوشته شده بسیار کم است زیرا هر گاه مطلبی افزوده، حذف و یا جایگزین شود این امر در نخستین نگاه و براحتی قابل کشف است. در مقابل، یک فایل الکترونیکی را به راحتی می‌توان تغییر داد، مگر آنکه به خوبی از آن محافظت شده باشد. با این وجود، هر تغییری که در فایل الکترونیکی صورت گیرد آثاری از خود بر جا می‌گذارد (مثلاً تغییر تاریخ یا ساعت فایل). به علاوه، امروزه امکان مقابله با این مشکل از طریق به کارگیری امضاهای دیجیتال فراهم آمده است.

۲ـ قابلیت خوانده شدن: آنچه را که بر روی کاغذ نوشته شده است باید بتوان براحتی و «بطور مستقیم» خواند. بنابراین، زبان به کار رفته جهت تهیه نوشته باید برای اشخاص ذینفع قابل فهم باشد، در غیر این صورت این اشخاص به مترجم مراجعه خواهند نمود؛ این واقعیت ما را بر آن می‌دارد تصدیق نماییم که نوشته الکترونیکی نیز، اگرچه به صورت غیر مستقیم، قابل خواندن است، زیرا با آنکه این نوع نوشته به زبان دودویی نگاشته شده که برای انسان قابل رؤیت و فهم نیست معذلک با به کارگیری ابزاری مناسب می‌توان آن را خواند.

۳ـ ثبات و دوام: نوشته کاغذی از ثبات و دوام کافی برخوردار است، معمولاً کاغذ با گذشت زمان از بین نمی‌رود. بدیهی است که این ویژگی در نوشته‌های الکترونیکی نیز وجود دارد و این نوع نوشته‌ها را می‌توان طی مدت زمان دلخواه نگهداری نمود.

۴ـ قابلیت انتساب نوشته به فرد معین: در صورتی که نوشته‌ی موجود بر روی کاغذ، امضاء شده باشد براحتی می‌توان نویسنده آن را شناسایی کرد و حتی در غیر اینصورت و در مواجهه با سند بدون امضاء نیز چنین امکانی فراهم است زیرا

۴۶- Inalterability

۴۷- Legibility

۴۸- Stability

۴۹- Identification

۵۰- Attributability

۵۱- D. Gobert et E.Montero,L'ouverture de la preuve littérale aux écrits sous forme électronique, P.124

با مراجعه به کارشناس می‌توان خط افراد را تشخیص داده و نوشته را به فرد معینی منسوب نمود، اما در خصوص اسناد الکترونیکی وضعیت به گونه‌ای دیگر است زیرا ماهیت مجازی این نوع اسناد مانع از آن است که براحتی آنها را متعلق به فرد خاصی بدانیم. با این وجود، در حال حاضر با استفاده از انواع معینی از امضاهای الکترونیکی (از جمله امضای دیجیتال) امکان شناسایی نویسنده اسناد الکترونیکی نیز وجود دارد.

ملاحظه می‌شود که نظریه «معادل‌های کارکردی» در ضمن بیان کارکردهای اساسی نوشته استدلال می‌کند که اسناد الکترونیکی نیز قابلیت ارایه این کارکردها را دارند و نتیجتاً می‌توان آنها را نیز به عنوان سند نوشته (مکتوب) تلقی نمود و به عنوان دلیل در دادرسی‌ها پذیرفت.

۳ـ امضاهای الکترونیکی

در این قسمت ابتدا مفهوم؛ و سپس انواع امضاهای الکترونیکی را بیان نموده و در نهایت توضیحاتی در خصوص امضای دیجیتال ارایه می‌نمائیم.

الف) مفهوم امضای الکترونیکی:

قانون نمونه امضاهای الکترونیکی آنسیترال در ماده۲ (الف) امضای الکترونیکی را بدین صورت تعریف کرده است: «داده‌های الکترونیکی که به یک داده پیام منضم شده یا به صورت منطقی با آن مرتبطند و از آنها می‌توان جهت شناسایی امضاکننده داده پیام و [نیز] تأیید وی در خصوص اطلاعات موجود در داده پیام استفاده نمود». در این تعریف به دو کارکرد مهم و عمده امضاء اشاره شده است: ۱ـ شناسایی امضاء کننده؛ ۲ـ قصد ملتزم شدن امضاءکننده به مفاد سند امضاء شده، که از آن می‌توان به عنوان عنصر معنوی امضاء یاد کرد.[۵۲]

دستورالعمل امضاهای الکترونیکی اتحادیه اروپایی در ماده۲ (۱) به‌طور کلی امضای ا لکترونیکی را چنین تعریف کرده: «داده الکترونیکی که به دیگر داده‌های الکترونیکی منضم شده و یا به صورت منطقی با آنها مرتبط است و به عنوان وسیله‌ای جهت مستندسازی به کار می‌رود». مطابق این تعریف هر تکنیکی که به تنهایی یا ضمن ترکیب با تکنیک‌های دیگر، کارکردهای امضا را ارایه دهد امضای الکترونیکی نامیده می‌شود[۵۳].

قانون یکنواخت مبادلات الکترونیکی آمریکا (ماده۲ (۸)) و قانون امضاهای الکترونیکی آلمان (ماده۲ (۱)) نیز تعاریف مشابهی از امضای الکترونیکی ارایه داده‌اند.

در فرانسه تا پیش از تصویب قانون ۱۳ مارس ۲۰۰۰ (و اصلاح قانون مدنی)، امضاء به عنوان علامت یا هر نماد دیگر نوشته شده توسط شخص متعهد شناخته می شد. اما قانون مذکور بدون توجه به شکل امضاء به کارکردهای آن اشاره کرده

۵۲– Professor Chris Reed, What is a signature, P.9

۵۳– Mireille Antoine, D. Gobert, La directive européenne sur la signature électronique, vers la sécurisation des transaction sur l'Internet?

است.[۵۴] بدین صورت که ماده ۴-۱۳۱۶ قانون مدنی در خصوص امضاء به صورت کلی بیان می دارد:«امضای ضروری جهت تکمیل عمل حقوقی، بیانگر هویت امضاءکننده است. [همچنین] امضا دال بر رضایت طرفین نسبت به تعهدات ناشی از این عمل حقوقی است». مطابق بند دوم ماده ۴ـ۱۳۱۶ قانون مدنی فرانسه «امضای الکترونیکی عبارت است از به کارگیری روشی مطمئن جهت شناسایی که ارتباط امضا را با سندی که به آن منضم شده تضمین می‌کند».

در ماده ۲ـ۹ قانون تجارت الکترونیکی جمهوری اسلامی ایران، آمده است: «امضای الکترونکی عبارت از هر نوع علامت منضم شده یا به نحو منطقی متصل شده به «داده پیام» است که برای شناسایی امضا کننده داده پیام مورد استفاده قرار می‌گیرد». همانطور که ملاحظه می‌شود در این ماده به عنصر معنوی امضاء یعنی قصد التزام امضا کننده به مفاد سند امضا شده اشاره‌ای نشده است.

ب) انواع امضاهای الکترونیکی:

ب – ۱) دسته بندی بر مبنای به کارگیری یا عدم به کارگیری رمزنگاری[۵۵]

با توجه به تعاریف عام ارایه شده از امضای الکترونیکی، تکنیک‌ها و مکانیسم‌های مختلفی در محدوده این تعریف قرار می‌گیرند. این مکانیسم و تکنیک ها را می‌توان به دو دسته تقسیم بندی کرد:

ب-۱-۱) امضاهای الکترونیکی مبتنی بر رمزنگاری[۵۶]: رمزنگاری شاخه‌ای از ریاضیات کاربردی[۵۷] است که موضوع آن تبدیل داده‌ها به رمز جهت نیل به ایمنی مطلوب است. در جریان رمزنگاری، فرستنده پیغام رمزنگاری نشده[۵۸] را به یک متن کدگذاری شده[۵۹] تبدیل می‌کند. دریافت کننده پیغام، رمزنگاری را برای یکی از مقاصد زیر به کار می‌برد: الف) تبدیل متن کذگذاری شده به شکل اصلی و رمزنگاری نشده آن؛ ب) تشخیص هویت فرستنده پیغام؛ ج) تشخیص تمامیت داده‌ها یا عدم آن؛ و یا ترکیبی از سه مورد ذکر شده. مطلوب‌ترین نوع از این امضاها، امضای دیجیتالی[۶۰] است که در صفحات بعدی توضیحاتی در خصوص آن ارایه خواهد شد.

۵۴- Isabelle de lamberterie, Jean-Francois Blanchette, Le décret du 30 Mars 2001, …., lecture critique, technique et juridique, P.3

۵۵- Uncitral model law on electronic signatures with guide to enctmant, Introduction to public key technology and the federal PKI infrastructure, Dr. Richard Kuhn et al.

۵۶- Cryptography

۵۷- applied mathematics

۵۸- Plaintext

۵۹- Coded text, Ciphertext

۶۰- Digital signature

ب-۱-۲)-امضاهای الکترونیکی غیر مبتنی بر رمزنگاری: همان طور که از عنوان این نوع امضاها بر می‌آید، وجه تمایز آنها با دسته نخست، استفاده نکردن از رمزنگاری در جریان به کارگیری آنها است. به عنوان یکی از مصادیق این نوع امضا،

می‌توان امضاهای رقمی[۶۱] شده را نام برد که از طریق اسکن کردن امضای دستی (سنتی) فرد ایجاد می‌شوند. فردی که تمایل دارد یک سند الکترونیکی را امضا کند، به این منظور، تصویر امضای خود را به کار گیرد.

نمونه دیگر از این نوع امضاها، مکانیسم‌های مبتنی بر «معرف‌های زیست شناختی[۶۲]» هستند. در این مکانیسم‌ها از یک خصیصه فیزیکی منحصر بفرد جهت معرفی و شناسایی امضا کننده استفاده می‌شود. از جمله مهمترین معرف‌های زیست شناختی می‌توان این موارد را ذکر کرد: اثر انگشت، امضاهای دستی، الگوی صوتی، الگوی تایپ‌کردن، حالت شبکیه چشم و...

ب-۲) تقسیم‌بندی بر مبنای سطح ایمنی فراهم شده

همانطور که ملاحظه کردیم تعریف دستورالعمل اتحادیه اروپا و دیگر تعاریف ارایه شده از امضای الکترونیکی به گونه‌ای تنظیم شده که تمام تکنیک‌هایی را دربرگیرد که کارکردهای امضای سنتی را ارایه می‌دهند و درواقع در این تعاریف نوعی «بی‌طرفی تکنولوژیک[۶۳]» اتخاذ شده و هیچ یک از مکانیسم‌های تولید امضای الکترونیکی بر دیگر مکانیسم‌ها برتری داده نشده است. دلیل این بی‌طرفی توجه به تنوع روش‌های تولید امضای الکترونیکی و پیشرفت‌های سریعی بوده که در این زمینه رخ می‌دهد[۶۴]. با اینحال در قوانین مختلف معمولاً پس از ارائه تعریفی کلی از امضای الکترونیکی، نوع خاصی از این امضاء ذکر شده که امتیازات ویژه‌ای برای آن در نظر گرفته شده است: امضای الکترونیکی پیشرفته[۶۵] یا امضای الکترونیکی ایمن[۶۶]، علت این امر آگاهی از این واقعیت است که همه امضاهای الکترونیکی از نظر حقوقی سطح یکسانی از امنیت را فراهم نمی‌آورند. برای نمونه تایپ کردن نام نویسنده در پایان یک پیغام الکترونیکی در قلمرو تعریف عامّ امضای الکترونیکی قرار می‌گیرد ولی هیچ تضمینی در خصوص حفظ تمامیت پیغام الکترونیکی دربرندارد.

در ماده ۲ـ۲ دستورالعمل امضاهای الکترونیکی اتحادیه اروپا، امضای الکترونیکی پیشرفته بدین صورت تعریف شده است: « امضای الکترونیکی پیشرفته امضای الکترونیکی است که شرایط ذیل را داشته باشد:

الف) به صورت انحصاری با امضاء کننده مرتبط باشد؛

۶۱- Digital signature

۶۲- Biometric Identifiers

۶۳- Technological Neutrality

۶۴- Sofian Azabi, ibid, P.5

۶۵- Advanced electronic signature

۶۶- Secure electronic signature

ب) شناسایی امضاء کننده را ممکن سازد؛

ج) از به کارگیری ابزاری ایجاد شده باشد که امضاء کننده بتواند آنها به طور انحصاری تحت کنترل خود درآورد؛ و

د) با داده‌هایی که به آنها مربوط می‌شود به صورتی مرتبط باشد که هر گونه تغییر بعدی در این داده‌ها قابل کشف باشد».

ماده ۱ـ۵ این دستورالعمل مقرر می‌دارد که تحت شرایط معینی امضای الکترونیکی به عنوان دلیل در دادگاه پذیرفته شده و از همان قدرت اثباتی امضای دستی (سنتی) برخوردار خواهد شد. مطابق ضمیمه ۳ دستورالعمل مذکور این شرایط عبارتند از اینکه: ۱ـ امضای الکترونیکی به مفهوم (ماده ۲ـ۲) پیشرفته باشد؛ ۲ـ مبتنی بر یک گواهی حائز شرایط (ماده ۵ـ۲) باشد؛ ۳ـ با استفاده از مکانیسمی ایمن (که ضمیمه ۳ دستورالعمل شرایط آن را بیان کرده) ایجاد شده باشد».

در فرانسه ماده ۲ـ۱ فرمان ۳۰ مارس ۲۰۰۱ شورای دولتی این کشور امضای الکترونیکی را که شرایط ذیل را داشته باشد امضای الکترونیکی ایمن می‌نامد: « ۱ـ به طور انحصاری متعلق به امضاکننده باشد؛ ۲ـ با استفاده از مکانیسم‌هایی تولید شده باشد که امضاءکننده بتواند آنها را تحت کنترل انحصاری خود بگیرد؛ و ۳ـ چنان رابطه‌ای بین این امضاء و متنی که به آن ضمیمه شده است برقرار باشد که تمام تغییرات بعدی سند قابل کشف باشند».

قانون تجارت الکترونیکی جمهوری اسلامی ایران در ماده ۱۰ شرایط زیر را برای امضای الکترونیکی مطمئن ضروری دانسته است: «۱ـ نسبت به امضاءکننده منحصر به فرد باشد؛ ۲ـ هویت امضاءکننده داده پیام را معلوم نماید؛ ۳ـ به وسیله امضاءکننده و یا تحت اراده انحصاری وی صادر شده باشد؛ ۴ـ به نحوی به یک داده پیام متصل شود که هر تغییری در آن داده پیام قابل کشف باشد».

در ماده ۱۵ قانون مذکور آمده است: «نسبت به داده پیام مطمئن، سوابق الکترونیکی مطمئن و امضای الکترونیکی مطمئن انکار و تردید مسموع نیست و تنها می‌توان ادعای جعلیت به داده پیام وارد و یا ثابت نمود که داده پیام مزبور به جهتی از جهات قانونی از اعتبار افتاده است».

قانون یکنواخت مبادلات الکترونیکی آمریکا (UETA) بین امضای الکترونیکی ساده و امضای الکترونیکی پیشرفته یا مطمئن تفکیکی قایل نشده است.

لازم به ذکر است که در حال حاضر صرفاً امضای دیجیتال شرایط امضای الکترونیکی پیشرفته، ایمن (و یا به تعبیر قانون تجارت الکترونیکی جمهوری اسلامی ایران امضای الکترونیکی مطمئن) را که در قوانین مختلف ذکر شده است دربردارد[۶۷] که در ذیل توضیح مختصری در خصوص آن ارایه می‌شود[۶۸]:

ج) امضای دیجیتال

امضاهای دیجیتال از طریق رمزنگاری ایجاد و شناخته می‌شوند. همانطور که گفتیم رمزنگاری شاخه‌ای از ریاضیات کاربردی است که موضوع آن تبدیل پیغام‌ها به شکل و صورتی است که در حالت عادی قابل فهم و خواندن نباشد، عکس این

۶۷- D. Gobert et E.Montero, ibid, P.116

۶۸- ABA Digital Singature Guidelines, pp.3-6

عملیات (یعنی قابل فهم کردن پیغام رمزنگاری شده) نیز با استفاده از این شاخه ریاضیات کاربردی امکان‌پذیر است. رمزنگاری مبتنی بر کلید عمومی،[۶۹] روشی است که در ایجاد امضاهای دیجیتال به کار می‌رود: در این نوع رمزنگاری از الگوریتمی استفاده می‌شود که شامل دو کلید متفاوت است؛ این دو کلید در عین حال از نظر ریاضی با هم مرتبط هستند. از بین این جفت کلید[۷۰]، یک کلید برای ایجاد امضای دیجیتال و یا تبدیل داده‌ها به شکلی نامرئی و غیرقابل فهم و کلید دیگر جهت شناسایی امضای دیجیتال و یا برگرداندن پیغام رمزنگاری شده به شکل اولیه آن به کار می‌رود. تجهیزات رایانه‌ای و نرم‌افزاری که از این دو کلید استفاده می‌کنند اغلب «سیستم رمزنگاری نا متقارن[۷۱]» نامیده می‌شوند.

دو کلید مکملی که از آنها در سیستم رمزنگاری نا متقارن استفاده می‌شود، کلید خصوصی[۷۲]– که صرفاً امضا کننده از آن مطلع است و برای ایجاد امضای دیجیتال به کار می‌رود– و کلید عمومی[۷۳]– که معمولاً افراد بیشتری آن را می‌شناسند و جهت شناسایی و بررسی اصالت و اعتبار امضای دیجیتال مورد استفاده قرار می‌گیرد– نامیده می‌شوند. اگر در اثر روابط گسترده امضا کننده با دیگران، اشخاص زیادی به شناسایی و بررسی اعتبار امضای دیجیتال امضا کننده نیاز داشته باشند، کلید عمومی باید بین تمامی آنها توزیع (و برای آنها ارسال) شود و یا در دسترس آنها باشد مثلاً از طریق درج در یک دفترچه راهنما یا فهرست برخط (on-line) که براحتی قابل دسترسی باشد. علیرغم ارتباط ریاضی کلیدهای این جفت کلید، در صورتی که سیستم رمزنگاری نامتقارن به صورتی ایمن طراحی و اجرا شده باشد، پی بردن به کلید خصوصی از طریق علم به کلید عمومی امری ناممکن خواهد بود. بنابراین، اگرچه ممکن است افراد بسیاری از کلید عمومی امضا کننده آگاه بوده و آن را جهت شناسایی امضای وی به کار گیرند، این افراد نمی‌توانند کلید خصوصی مشارالیه را کشف نمود. و برای جعل امضای دیجیتال وی از آن استفاده کنند.

ج-۱) عملیات خردسازی[۷۴]

فرآیند مهم دیگری که اصطلاحاً «کارکرد (عملیات) خرد سازی» نامیده می‌شود، جهت ایجاد و شناسایی امضای دیجیتال به کار گرفته می‌شود. عملیات خردسازی شامل الگوریتمی است که شکل یا (به اصطلاح) «اثرانگشت[۷۵]» دیجیتال از پیغام را به صورت یک «ارزش خرد[۷۶]» و یا «نتیجه خرد[۷۷]» با اندازه‌ای استاندارد ایجاد می‌کند که معمولاً از پیغام بسیار کوچک تر بوده

۶۹- Public key Cryptogrphy

۷۰- Key Pair

۷۱- Asymetric Cryptography

۷۲- Private Key

۷۳- Public Key

۷۴- Hash functio

۷۵- Digital Fingerprint

۷۶- Hash Value

۷۷- Hash Result

ولی با این وجود نسبت به آن منحصر بفرد است. هرگونه تغییری در پیغام، لاجرم، نتیجه خرد متفاوتی را، در صورت انجام همان عملیات خردسازی که بر روی پیغام صورت گرفته، در پی خواهد داشت. هرگاه یک عملیات خردسازی ایمن، که اصطلاحاً «عملیات یکطرفه خردسازی[۷۸]» نامیده می‌شود، به کار رود، تشخیص و کشف پیغام اولیه از طریق علم به ارزش خرد آن غیرممکن خواهد بود. بنابراین عملیات خردسازی، نرم‌افزار ایجاد کننده امضای دیجیتال را قادر می‌سازد که بر روی مقادیر کوچک‌تری از داده‌ها عمل نماید و در عین حال دلیلی محکم مبنی بر ارتباط دو طرفه میان پیغام اصلی و شکل خرد شده آن فراهم آورده و از این طریق به نحو مطلوبی تضمین می‌نماید که از زمان امضا شدن به صورت دیجیتال، هیچگونه تغییری در پیغام حاصل نشده است. بنابراین، و به طور معمول،استفاده از امضاهای دیجیتال شامل دو فرآیند است، که یکی از آنها توسط امضا کننده و دیگری به وسیله دریافت کننده امضای دیجیتال صورت می‌گیرد:

الف) ایجاد امضای دیجیتال: در این فرآیند از شکل خرد شده پیغام اصلی استفاده می‌شود که هم نسبت به پیغام امضا شده و هم نسبت به کلید خصوصی منحصر به فرد است. در حقیقت، این مرحله شامل امضای پیغام خرد شده به وسیله کلید خصوصی است.

ب) شناسایی امضای دیجیتال: که شامل فرآیند چک کردن امضای دیجیتال به وسیله مراجعه به پیغام اصلی و استفاده از یک کلید عمومی مشخص است. از این طریق می‌توان تعیین نمود که آیا امضای دیجیتال برای امضا کردن پیغام موردنظر و با استفاده از کلید خصوصی مرتبط با کلید عمومی موجود در دسترس دریافت کننده، ایجاد شده یا خیر.

ج-۲) مراجع گواهی[۷۹]

دریافت کننده امضای دیجیتال جهت شناسایی و تشخیص اصالت و اعتبار امضای دیجیتال، باید به کلید عمومی امضاکننده دسترسی داشته و اطمینان یابد که این کلید با کلید خصوصی امضا کننده هماهنگ و مرتبط اســت. با این وجود، جفت کلید عمومی و خصوصی، هیچگونه ارتباطی با شخص خاصی نداشته و صرفاً مجموعه‌ای از ارقام هستند. به منظور مرتبط نمودن این جفت کلید به یک شخص معین (اعم از حقیقی یا حقوقی) اتخاذ تدابیر مناسبی لازم است.

در مبادله‌ای که صرفاً دو طرف در انجام آن نقش دارند، هر یک از طرفین می‌تواند کلید عمومی از جفت کلیدی را که به کار خواهد برد به اطلاع طرف مقابل برساند (مثلاً از طریق پست و یا یک مکالمه تلفنی ایمن). اما انجام چنین کاری چندان هم ساده نیست، به ویژه در مواردی که طرفین از نظر جغرافیایی در فاصله بسیار طولانی از هم قرار داشته و به طور معمول، از طریق ابزاری مطلوب و به صرفه اما ناامن مانند اینترنت با یکدیگر ارتباط برقرار نموده و علاوه بر این اشخاص حقیقی نبوده و شرکت‌های تجاری یا شخصیت‌های حقوقی دیگری هستند. همگام با گسترش استفاده از اینترنت، مبادلات مهمی (اعم از تجاری و غیر آن) بر روی این شبکه و میان بیگانگانی صورت خواهد گرفت که هیچگونه رابطه قراردادی سابقی نداشته و چه

۷۸- One- way Hash functio

۷۹- Certification Authorities

بسا هیچگاه دوباره با یکدیگر معامله ننمایند. با عنایت به این واقعیت، اهمیت تصدیق امضای دیجیتال اشخاص به خوبی بر ما نمایان می‌شود.

در این راستا، ممکن است امضا کننده اظهاریه‌ای عمومی صادر کرده و مثلاً طی آن بیان دارد: «امضاهایی که به وسیله کلید عمومی ذیل قابل شناسایی باشند، به اینجانب تعلق دارند». با این وجود، اشخاصی که با امضاکننده ارتباط برقرار می‌کنند حق خواهند داشت از پذیرش چنین اظهاراتی امتناع نمایند، به ویژه درمواردی که طرفین قبلاً قراردادی را به صورت الکترونیکی منعقد ننموده اند تا اثر قانونی این اظهارات را تثبیت نماید. طرفی که در یک سیستم باز ارتباطی مانند اینترنت به چنین اظهارات غیر موثق و تأیید نشده‌ای اطمینان کنند با خطر بزرگ اعتماد به فردی متقلب و حقه باز مواجه خواهند بود. راه حلی که در این خصوص مفید به نظر می‌رسد، استفاده از خدمات یک یا چند شخص ثالث موثق[۸۰] را است که تعلق کلید عمومی را به یک امضاکننده معین تصدیق نماید. این شخص ثالث موثق مرجع گواهی نامیده می‌شود.

جهت تصدیق تعلق جفت کلید به امضا کننده، مرجع مزبور یک گواهی (سند) الکترونیکی صادر می کند که در آن کلید عمومی به عنوان «موضوع گواهی[۸۱]» مشخص شده و تصدیق می‌نماید که امضا کننده معرفی شده در گواهی، کلید خصوصی مرتبط با این کلید عمومی را در اختیار دارد. امضا کننده معرفی شده در گواهی اصطلاحاً «مشترک[۸۲]» نامیده می‌شود. کارکرد اصلی و عمده گواهی تصدیق تعلق جفت کلید به یک مشترک معین است. مرجع گواهی نیز جهت معرفی خود و اثبات اصالت گواهی، آن را به صورت دیجیتال امضا می‌کند. به منظور شناسایی امضای دیجیتال مرجع مذکور و اطمینان از اصالت و اعتبار آن می‌توان کلید عمومی مرجع گواهی را بکاربرد. بدیهی است که تعلق این کلید به مرجع گواهی نیز باید توسط مرجع دیگری و از طریق صدور یک گواهی دیجیتال صورت پذیرد. این روند همچنان ادامه خواهد یافت تا آن که شخصی که به امضای دیجیتال اعتماد نموده نهایتاً نسبت به اصالت و اعتبار آن اطمینان یابد.

در قوانین مختلف شرح وظایف و مسوولیت های مراجع گواهی (اعم از قراردادی و قهری) به تفصیل بیان شده که بحث از آن مجال فراخ تری می‌طلبد. باب دوم قانون تجارت جمهوری اسلامی ایران به دفاتر خدمات صدور گواهی الکترونیکی اختصاص یافته و ماده ۳۱ قانون مذکور این دفاتر را واحدهایی می‌داند «که برای ارائه خدمات صدور امضای الکترونیکی در کشور تأسیس می‌شوند. این خدمات شامل تولید، صدور، ذخیره، ارسال، تأیید، ابطال و به روز نگهداری گواهی‌های اصالت (امضای) الکترونیکی می‌باشد». در ماده ۳۲ همان قانون نیز تهیه آیین نامه و ضوابط نظام تأسیس و شرح وظایف این دفاتر بر عهده سازمان مدیریت و برنامه‌ریزی کشور و وزارتخانه‌های بازرگانی، ارتباطات و فناوری اطلاعات، امور اقتصادی و دارائی و دادگستری گذاشته شده که هیأت وزیران آن را تصویب خواهد نمود.

۸۰- Trusted Third Paryt

۸۱- Certification Subject

نتیجه‌گیری

انجام مبادلات مختلف (اعم از تجاری و ...) به صورت الکترونیکی همچنان در حال گسترش است و تاکنون در این خصوص قوانین و مقررات مختلفی وضع شده که هدف از تمامی آنها تسهیل و ایمن‌سازی مبادلات الکترونیکی بوده است، زیرا در صورت فقدان اصول و ضوابط مناسب، فعالیت‌های تجاری از این نوع با وقفه و اختلال مواجه شده و به تبع آن اشخاص روش‌های سنتی را بر تجارت الکترونیکی ترجیح خواهند داد. قانون تجارت الکترونیکی جمهوری اسلامی ایران مصوب ۱۳۸۲/۱۰/۱۷ گامی است مهم در جهت توسعه مبادلات الکترونیکی و نظام بخشیدن به آن که در عین حال نیازمند تأمل و تعمق بیشتر و اصلاحاتی است که نیل به آن جز از طریق مطالعه دقیق‌تر منابع موجود در این خصوص، ممکن نخواهد بود. امیدواریم که اساتید و دانشجویان علاقه‌مند به رشته‌های جدیدی مانند تجارت الکترونیکی (که تلفیقی است از مسایل حقوقی و فنی) با گسترش مطالعات و ارایه آثار خود راه را برای شکوفایی هر چه بیشتر این رشته نوین هموارتر نمایند.

منابع و مآخذ

الف) به زبان فارسی

۱) بختیاروند، مصطفی (مترجم)، چارچوب تجارت الکترونیکی (رویه تقنینی بین‌المللی)، خبرنامه انفورماتیک شماره ۸۷
۲) بختیاروند، مصطفی (مترجم)، قانون نمونه امضاهای الکترونیکی آنسیترال، خبرنامه انفورماتیک – شماره ۸۸
۳) بختیاروند، مصطفی(مترجم)، قانون نمونه تجارت الکترونیکی آنسیترال، خبرنامه انفورماتیک – شماره ۸۹
۴) زرکلام، ستار، امضای الکترونیکی و جایگاه آن در نظام ادله اثبات دعوی، فصلنامه علمی ـ پژوهشی دانشکده علوم انسانی (حقوقی) دانشگاه تربیت مدرس، بهار ۱۳۸۲، صص ۵۶ ـ ۳۳
۵) شهیدی، مهدی، تشکیل قراردادها و تعهدات، نشر حقوقدان
۶) کاتوزیان، ناصر، قواعد عمومی قراردادها، جلد اول، شرکت سهامی انتشار
۷) کاتوزیان، ناصر، عقود معین، جلد اول، شرکت سهامی انتشار
۸) نوری، نخجوانی، حقوق تجارت الکترونیکی، کتابخانه گنج دانش
۹) مصطفوی،حجت الاسلام دکتر سید مصطفی، جزوه درسی فقه (۳)، دانشگاه امام صادق (ع)
۱۰)صفایی، سیدحسین، جزوه درسی حقوق مدنی (۹)، دانشگاه امام صادق(ع)

ب) به زبان انگلیسی

1. Tomas J. Smedinghoff, The legal requirements for creating secure and enforceable electronic transactions.
2. Christine Hart, online dispute resolution and avoidance in electronic commerce
3. Alan Gahtan, Electronic Evidence
4. ABA Digital Signature Guidelines, WWW.abanet.org
5. UNCITRAL Model law on electronic commerce with guide to enactment, WWW. uncitral. Org
6. UNCITRAL Model law on electronic signature with guide to enactment, WWW.Uncitral.org
7. US Uniform Electronic Transactions Act (UETA)
8. Directive 2000/31/EC of the European parliament and the council of june 2000 on electronic commerce
9. Directive 1999/93/EC of the European parliament and the council of December 1999 on a community framework for electronic signature.
10. Directive 95/46/EC of the European parliament and the council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, WWW.bka.gv
11. WWW.info.gov.hk
12. Germany Electronic Signature Statute
13. Professor chris Reed, What is a signature
14. Introduction to public key technology and the fedral PKI infrastructure,Dr.Richard Kuhn et al.
15. Michael Chissick,Alistair Kelman,Electronic Commerce,Law and Practice

ج) به زبان فرانسه

1- Mireille Antoine et Didier Gobert, la directive européenne sur la signature électronique, Vers la sécurisation des transaction sur l'Internet?
2- Isabelle de lamberterie et Jean-Francois Blanchette, le décret du 30 mars 2001, relatif à la signature électronique: lecture critique, technique et juridique.
3- Didier Gobert et Etienne Montero, la signature dans les contrats et les paiements électroniques, l'approache fonctionnelle
4- Didier Gobert et Etienne Montero, l'ouvertrue de la preuve littérale aux écrits sous forme électronique
5- Sofian Azzabi, le nouveau régime probatoire francais

☑ **عنوان: بررسی ماهیت حقوقی حق امتیاز شیرینک رپ**

☑ **نویسنده: محمد مهدی حسن پور**

مبحث اول: معرفی

۱ـ معرفی قراردادهای انفورماتیک

یکی از شاخه‌های حقوق فن‌آوری اطلاعات ((information technology(IT))، قراردادهای انفورماتیک می‌باشد. معادل فرانسوی این واژه contrat informatique و معادل انگلیسی آن computer contract می‌باشد. به همین جهت است که به این قراردادها قراردادهای کامپیوتری هم گفته می‌شود. قراردادهای انفورماتیک قراردادهایی هستند بین شرکت نرم‌افزاری و شرکت مشتری که موضوع آن خرید و فروش سخت‌افزار و نرم‌افزار، خدمات انفورماتیک شامل خدمات پشتیبانی، مدیریت امکانات و خدمات اینترنتی می‌باشد.

ممکن است این سؤال در ذهن هر خواننده‌ای ایجاد شود که چه ویژگی در این نوع قراردادها باعث شده که بطور اختصاصی مطرح شوند و مورد بررسی قرار گیرد؟ این ابهام را این واقعیت تأیید می‌کند که قراردادهای انفورماتیک را نباید با قراردادهای on-line اشتباه گرفت: قراردادهای on-line به کلیه معاملاتی می‌گویند که در فضای اینترنت انجام می‌شود مشتری با مراجعه به سایت فروشنده ایجاب فروش کالایی را قبول کرده و با کارت اعتباری‌اش پرداخت می‌کند. به عبارت دیگر قراردادهای on-line یک روش انجام معامله است همین معامله ممکن است به صورت شفاهی یا کتبی باشد که دیگر به آن on-line نمی‌گویند با این توضیح روشن شد که خود قراردادهای انفورماتیک ممکن است به صورت کتبی و کاغذی یا شفاهی و یا on-line باشد. زمانی که شما یک مانیتور کامپیوتر را از مغازه فروش لوازم رایانه‌ای تهیه می‌کنید قرارداد کتبی می‌بندید ولی اگر همین قرارداد را را مراجعه به سایت فروش لوازم رایانه‌ای انجام دهید معامله شما on-line خواهد بود.

با این توضیح سراغ سؤال اول می‌رویم که ویژگی‌های که باعث می‌شوند قراردادهای انفورماتیک مستقلاً مورد بررسی و تحلیل قرار بگیرند چیست؟ بنظر اینجانب سه ویژگی در این قراردادها وجود دارد که مقتضی بررسی مستقل این قراردادها است البته این به معنی رها کردن اصول و قواعد عمومی قراردادها در این خصوص نیست بلکه منظور تخصصی شدن این قراردادها می‌باشد. ویژگی اول کاربرد بالای آن است ما در عصر اطلاعات زندگی می‌کنیم عصری که در آن منابع مادی و انسانی حرف اول را نمی‌زند بلکه کشوری قدرتمندتر است که اطلاعات بیشتری داشته باشد. بعینه رشد استفاده از رایانه و لوازم رایانه‌ای را در جامعه می‌بینیم رابطه حقوقی که بین مشتری و فروشنده، مشتری و خدمات دهنده درکلیه این موارد برقرار می‌شود در چهارچوب قراردادهای انفورماتیک مطرح است.

ویژگی دوم: پیچیدگی این قراردادها است: از یک طرف تنظیم‌کننده قرارداد بایستی آشنایی لازم به نهادها و مفاهیم حقوقی کشور متبوع طرفین داشته باشد و از طرف دیگر بایستی تخصص فنی لازم در مورد سخت‌افزارها، نرم‌افزارها و خدمات موضوع معامله داشته باشد.

ویژگی سوم: وجود نرم‌افزار در این نوع معاملات بعنوان موضوع معامله است. نرم‌افزار شیء است غیر ملموس و غیر مادی که جز بوسایل خاص قابل رؤیت نیست. حق مؤلف بر نرم‌افزار سیستم سنتی تقسیم حقوق به عینی و دینی یا شخصی را بهم زده و حقی را بوجود آورده که بواقع نه عینی است نه دینی.

قراردادهای انفورماتیک انواع مختلفی دارند. در زیر جهت آشنایی خوانندگان برخی از این قراردادها را ذکر می‌کنیم:

- **قرارداد تهیه نرم‌افزار:** قراردادی است که با هدف تهیه برنامه‌های رایانه‌ای با مؤلف، تولید کننده، توزیع کننده و یا شرکت نرم‌افزاری بسته می‌شود. در تهیه نرم‌افزارباید دقت شود نرم‌افزار مورد نظر با سخت‌افزار مربوطه متناسب باشند.
- **قرارداد تهیه سخت‌افزار:** قراردادی است که با هدف تهیه تجهیزات سخت‌افزاری مثل مانیتور، کیس، صفحه کلید با تولید کننده، توزیع کننده یا شرکت نرم‌افزاری بسته می‌شود.
- **قرارداد پشتیبانی:** براساس این قرارداد پشتیبان تعهد می‌کند تجهیزات خاصی در شرایط مناسبی کار کنند و در صورت بروز اشکال وی آنرا تعمیر کند. گاه پشتیبان تعهد می‌کند برنامه نرم‌افزاری خاصی را تقویت کند یا گسترش دهد، اشکال‌ها و خطاهای آنرا رفع کند و نرم‌افزار را با جدیدترین نسخه آن جایگزین کند.
- **قرارداد آزمایش (تست):** این قرارداد مشخص می‌نماید سخت‌افزار یا نرم‌افزار خریداری شده باید چه آزمایشاتی را با موفقیت پشت سر بگذارد. اغلب از دو نوع آزمایش استفاده می‌شود: ۱ـ آزمایش آزمایشگاهی موسوم آنها ؛ ۲ـ آزمایش در محل نصب موسوم به بتا
- **قرارداد مدیریت امکانات یا برون‌سازی:** بیشتر شرکت‌ها از این قرارداد جهت خلاص شدن از بخش IT شرکت و واگذار کردن وظایف آن به یک شرکت خارجی استفاده می‌کنند.
- **قرارداد خدمات اینترنتی:** خدمات دهنده بدین وسیله تعهد می‌کند خدماتی از قبیل امکان جستجو، نسخه‌برداری از داده‌های آن‌لاین، وارد کردن داده به اینترنت، امکان پست الکترونیکی و طراحی سایت را در اختیار مشتری بگذارد.
- **قرارداد توزیع و بازاریابی:** قرارداد توزیع و بازاریابی قراردادی است که بدان وسیله تولیدکنندهٔ محصول یا خدمات خاصی فروش و عرضه محصولات خود را به شخص دیگری واگذار می‌نماید. این شخص اگر مستقل باشد توزیع کننده نام دارد و اگر وابسته به تولیدکننده باشد نماینده وی تلقی می‌شود.

یکی از قراردادهای انفورماتیک متداول در توزیع نرم‌افزار قرارداد حق امتیاز شرینک رپ است که در این مقاله مورد بررسی و تحلیل قرار خواهند گرفت.

۲ـ معرفی قرارداد حق امتیاز شرینک رپ

نرم‌افزار بعنوان جزئی از اجزاء رایانه را می‌توان به مجموعه دستوراتی تعریف کرد که به جزء فیزیکی رایانه یعنی سخت‌افزار فرمان می‌دهد. نرم‌افزار به اعتبار انواع رایانه از نظر کوچکی و بزرگی به سه قسم تقسیم می‌شود؛ نرم‌افزار مین فریم (main frame) ، نرم‌افزار مینی فریم (mini frame) و نرم‌افزار میکرو رایانه (micro computer). نرم‌افزارهای مینی و مین فریم در مورد رایانه‌هایی که برای مقاصد خاصی استفاده می‌شود کاربرد دارند. لذا بدیهی است که تولید و فروش آنها در سطح پایینی انجام شود. از همین رو قرارداد تهیه این نوع نرم‌افزارها معمولاً از طریق مذاکره متقابل و چانه‌زنی بر سر مفاد قرارداد تنظیم شده و به امضاء طرفین می‌رسد. در مقابل نرم‌افزار میکرو رایانه در رایانه‌های شخصی یا خانگی (PC) کاربرد دارد. این نرم‌افزار هم به نوبه خود به دو قسم تقسیم می‌شود. نرم‌افزار سفارشی و نرم‌افزار عمومی. نرم‌افزار سفارشی (bespoke software یا Custom.software) نرم‌افزاری است که به سفارش خریدار توسط نویسنده ساخته می‌شود و تولیدآن در سطح انبوه و گسترده نمی‌باشد. بدیهی است انتقال این نوع نرم‌افزار، مثل نرم‌افزارهای مینی و مین فریم، با قرارداد ویژه‌ای که حاصل چانه‌زنی و مذاکره طرفین است انجام می‌شود. در مقابل نرم‌افزار عمومی (Mass market software یا Pakaged software) است که در سطح انبوه تولید می‌شود و مورد نیاز هر کس است که یک دستگاه رایانه شخصی داشته باشد. در این مقاله لغت نرم‌افزار ناظر بر همین نوع می‌باشد. این نوع نرم‌افزارها در دو شکل نرم‌افزار سیستم عامل (مثل نرم‌افزار windows یا (Ms-Dos) و نرم‌افزار کاربردی Utility (مثل نرم‌افزار آنتی‌ویروس) وجود دارند. بدلیل کثرت فروش این نوع نرم‌افزارها و قیمت ارزان آن در مقایسه با سایر نرم‌افزارها برای تولید کننده بصرفه نیست که با تک‌تک خریداران قرارداد مستقلی امضاء کند یا امضاء قرارداد را از طریق نمایندگان خود به انجام رساند. بلکه تولیدکننده این نرم‌افزارها را به توزیع‌کننده‌ها و خرده‌فروش‌ها می‌فروشند و آنها نیز به نوبه خود با واسطه دیگری یا با کاربر نهایی (end user) وارد معامله می‌شوند.

برای اینکه کاربر بتواند از نرم افزار بهره‌برداری کند و در مقابل حقوق پدیدآورنده نرم‌افزار هم حفظ شود این سیستم توزیع کافی بنظر نمی‌رسد علت آن هم روشن است چون فروش نرم‌افزار متفاوت از فروش اتومبیل یا اسباب و اثاثیه منزل است. حقی که مالک اتومبیل بر آن دارد حقی است عینی که با فروش اتومبیل به دیگری کلیه حقوق وی من جمله حق مالکیت زایل می‌شود و به مشتری انتقال می‌یابد. بالعکس نرم افزار یک اثر فکری است که پدید آورنده آن علاوه بر حق مادی حق معنوی هم بر آن دارد[۱]. یعنی درست همانطور که نویسنده یک کتاب حق دارد از کتاب خود بعنوان مظهر شخصیت خود در مقابل انتقادات و اتهامات دفاع کند نویسنده نرم‌افزار نیز چنین حقی دارد. بنابراین حق نویسنده و مالک نرم‌افزار بر اثر فکری خود یک حق غیر عینی (intangible) است. پس تنها کس که حق استفاده از آنرا دارد خودش است و دیگران تنها زمانی این حق را پیدا می‌کنند که از نویسنده به آنها انتقال داده شود.

قرارداد حق امتیاز (license) قراردادی است که می‌خواهد حق بهره‌برداری از نرم‌افزار خریداری شده را به مشتری اعطا کند. پس قرارداد حق امتیاز نرم‌افزارهای عمومی قراردادی است بدون امضاء نویسنده به صورت نمونه (standard form) که به خریدار حق بهره‌برداری (use) از نرم‌افزار خریداری شده را اعطاء می‌کند.

قراردادهای معمول از این نوع به سه شکل هستند:

- قراردادهای حق امتیاز شرینک رپ (Shrink Wrap)

- قرارداد حق امتیاز کلیک رپ (Click Wrap)
- قرارداد حق امتیاز بِروز رپ (Browse Wrap)

اگرچه آنچه موضوع این مقاله است قرارداد شرینک رپ می‌باشد ولی از آنجا که این هر سه از یک خانواده‌اند و از نظر محتوا یکسان می‌باشند و تنها تفاوت آنها از نظر نحوه انعقاد و میزان اعتبار آنها می‌باشد، در مبحث معرفی سعی شده ضمن معرفی هر سه نوع بر قراردادهای کلیک‌رپ و بروزرپ تأکید بیشتری شود.

شرینک رپ (Shirnk Wrap) در لغت یعنی «در نایلون بسته‌بندی شده». در این قرارداد، قرارداد امتیاز بهره‌برداری از قبل نگاشته شده و در بسته‌بندی‌هایی که قالب نرم‌افزاری را در خود جای می‌دهند (دیسکت CD-Rom) با اسناد و مدارک احتمالی‌اش ارائه می‌شود. این مجموعه غالباً با اصطلاح انگلیسی "package" یعنی بسته مشخص می‌شود[۲].

این مجموعه با یک نایلون پوشیده شده که بطور برجسته روی آن نوشته شده (یا باید نوشته شده باشد) که (مثلاً) باز کردن بسته‌بندی بمعنی قبول شروط قرارداد حق امتیاز است[۳].

بنابراین می‌توان قرارداد شرینک‌رپ را اینگونه تعریف کرد که قرارداد حق امتیاز امضاء نشده‌ای است که اظهار می‌دارد قبولی کاربر نسبت به شروط قرارداد با پاره کردن نایلون و باز کردن بسته‌بندی نرم‌افزار یا با استفاده از نرم‌افزار یا با روش دیگری اعلام می‌شود. البته آنچه بیشتر معمول است استفاده از کلمه «باز کردن و پاره کردن» نایلون می‌باشد.

شروط این قرارداد ممکن است همگی از طریق نایلون قابل رؤیت باشند یا نباشند. آنچه در حال حاضر مرسوم است قسم دوم است. چرا که به علت کثرت شروط قراردادی و اقتضائات تجاری روش اول عملی نیست.

در هر حال، با توجه به کلیه منابعی که در نوشتن این مقاله مورد استفاده قرار گرفته‌اند، بنظر می‌رسد تعریفی که در کتاب برخی از نویسندگان[۴] از این نوع قرارداد آمده است تعریف درستی نباشد و با واقعیت موجود مطابقت ننماید.

این کتاب قرارداد شرینک‌رپ را به عنوان قراردادی معوض که مطلقاً کلیّه شروط آن از طریق نایلون قابل رؤیت می‌باشند تعریف کرده است.

در مقابل قرارداد شرینک رپ دو قرارداد کلیک رپ و بِروز رپ قرار د ارند وجه تمایز آنها این است که برخلاف قرارداد شرینک رپ، دو تای دیگر در زمره قراردادهای on-line هستند و در قلمرو تجارت الکترونیک (electronic commerce) جای می‌گیرند. به عبارت دیگر اولی قراردادی off-line است ولی دو تای دیگر on-line هستند و بوسیله اینترنت انجام می‌شوند.

لغات کلیک رپ و بروز رپ در حقیقت ابداع دادگاه‌هایی است که این اسامی را از شرینک رپ اقتباس کرده‌اند[۵].

در قرارداد کلیک رپ (Click Wrap) مشتری به صفحه وب فروشنده نرم‌افزار در اینترنت رفته و با پرداخت قیمت بصورت اعتباری آنرا در رایانه شخصی خود دان لود (down load) می‌کند. قرارداد کلیک رپ دو ویژگی دارد: اول آنکه مشتری را موظف می‌کند برای اینکه بتواند نرم‌افزار را به‌طور کامل نصب کند ابتدا شروط قرارداد حق لیسانس را بخواند دوم آنکه تکمیل عملیات نصب کامل جز بوسیله کلیک کردن بر دگمه «موافقم» یا «بله» که در ذیل آمده است ممکن نیست[۶]. به عبارت دیگر در پایان ذکر شرایط قرارداد حق امتیاز عبارتی به این مضمون آمده است: «آیا قرارداد حق امتیاز فوق را قبول می‌کنید؟ اگر

چنین است بر روی واژه «بله» و اگر چنین نیست بر روی واژه «خیر» کلیک کنید. عملیات set up تنها در صورتی ادامه می‌یابد که شما بر روی کلمه «بله» کلیک کنید.[۷]»

بنابراین می‌توان قرارداد کلیک رپ را چنین تعریف کرد که «قرارداد حق امتیازی است که درست بعد از نصب نرم‌افزار به صورت یک صفحه وب به نمایش درمی‌آید و کاربر را ملزم می‌نماید قبل از استفاده با کلیک بر دگمه «موافقم» رضایت خود را اظهار کند[۸]. در کامن لا به این نوع ابراز رضایت «اظهار رضایت»(to manifest assent) می‌گویند.

قرارداد حق امتیاز بروز رپ (Browse Wrap) هم از نظر محتوا با دو تای قبلی مشابه است و تفاوت آن با قرارداد کلیپ رپ آن است که در این نوع قرارداد مشتری مجبور و ملزم نیست برای اینکه بتواند نرم‌افزار را دانلود و نصب کند حتماً با کلیک بر دگمه‌ای رضایت خود را اظهار کند. وی می‌تواند مفاد این قرارداد را از طریق لینکی که در کنار علامت download قرار داده شده مشاهده کند. لغت بروز رپ (Browse Wrap) اشاره به هشداری دارد که روی صفحه وب قرار داده شده و به مشتری هشدار می‌دهد که استفاده از آن مشروط به قرارداد حق امتیازی است که، نه بر روی همان صفحه، بلکه بر روی صفحه دیگری قابل رؤیت می‌باشد و برخلاف قرارداد کلیک‌رپ این هشدار کاربر را موظف نمی‌کند قبل از دان‌لود کردن، نصب کردن یا استفاده کردن دگمه‌ای را کلیک کند[۹].

برخی شروط متعارف در قراردادهای حق امتیاز on-line عبارتند از: نحوه قبولی، توصیف خدمات، محدودیت استفاده شخصی و غیر تجاری، اشاره به نرم‌افزارهای خاصی که در این سایت قابل دسترسی است، اشاره به اسناد خاصی که در این سایت قابل دسترسی است، حساب اعضاء و کلمه رمزها و امنیت آن، ممنوعیت بهره‌برداری غیر قانونی، بهره‌برداری از خدمات، اشاره به اقامه دعوی نقض حق مؤلف در صورت تخلف، لینک‌هایی به سایت‌های اشخاص ثالث، تأکید بر حق مؤلف و علائم تجاری[۱۰].

در نهایت آنچه راجع‌به این سه نوع قرارداد لازم به ذکر است این مطلب است که این سه از نظر درجه اعتبار یکسان نیستند و به دلایلی که بعداً خواهیم گفت قرارداد کلیک رپ از باقی معتبرتر و قرارداد بروز رپ نسبت به باقی اعتبار کمتری دارد. در قسمت اعتبار قرارداد شرینک رپ بیشتر در این باره سخن خواهیم گفت.

در این مقاله ابتدا فواید و اهداف قرارداد شرینک رپ را ذکر می‌کنیم و سپس به مسأله اعتبار قرارداد شرینک رپ خواهیم پرداخت. قسمت اعتبار مهم‌ترین مبحث در رابطه با این قرارداد هست بطوری که دادگاه‌ها، وکلا و دانشجویان در مواجهه با این مسأله دو گروه شده‌اند برخی این قرارداد را نافذ و برخی آنرا غیر نافذ و باطل شمرده‌اند. در رابطه با اعتبار این قرارداد اشکالات زیادی به چشم می‌خورد که ما ابتدا این اشکالات را برمی‌شمریم و سپس هر کدام را در قسمت مربوطه مطرح می‌کنیم: چطور قبول مشتری نسبت به مفاد قرارداد حق امتیازی که از آن آگاهی ندارد ممکن است صحیح و تشکیل قراردادی را بدهد؟ طرفین قرارداد شرینک رپ چه کسانی هستند؟ آیا قراردادی با سه نفر متصور است؟ از نظر ماهیت حقوقی آیا یک قرارداد است یا دو قرارداد یکی بیع و یکی حق امتیاز؟ آیا این مسأله که موجب بتواند نحوه قبول را تعیین کند خلاف قواعد نیست؟ آیا این مسأله که قبول مشتری به اطلاع موجب نمی‌رسد خللی به قاعده لزوم اطلاع موجب از قبول نمی‌زند؟ یکی از ارکان هر عقدی وجود عوض است در حالیکه در عقد شرینک رپ اغلب عوضی برای کاربر متصور نیست؟ آیا بر مبنای رعایت تعادل بین متعاملین و با توجه به اینکه شروط عقد همگی بر کاربر تحمیل می‌شود و وی چاره‌ای جز پذیرش یا عدم پذیرش عقد ندارد نباید عقد را باطل دانست؟ زمانی که براساس قانون یک کاربر مجاز می‌تواند بدون نیاز به هر گونه قراردادی از نرم‌افزارخریداری شده استفاده کند

دادن اجازه استفاده بوسیله قرارداد چه معنی می‌تواند داشته باشد؟ بعلاوه زمانی که مشتری قانوناً حقوقی را کسب می‌کند آیا سلب کردن این حقوق از وی بوسیله قرارداد مشروع است؟

مبحث دوم: فواید قرارداد حق امتیاز شرینک رپ

در بررسی منابع مختلف هر کدام فوایدی برای این قرارداد برمی‌شمارند که ذیلاً آنها را ذکر کرد تحلیل می‌کنیم.

۱ـ اعطای امتیاز بهره برداری به کاربر

۲ـ تضمین حقوق مالکیت فکری نویسنده نرم‌افزار[۱۱]

۳ـ خنثی کردن نظریه اولین فروش (First sale doctrine)

در حقوق مالکیت فکری این نظریه به چشم می‌خورد که حق مؤلف نسبت به همان نسخه اثرش با فروش آن نسخه از اثر خود به خود زایل شده و به انتقال گیرنده یا مشتری بعنوان مالک نسخه فروخته شده انتقال می‌یابد. وی می‌تواند بدون آنکه لازم باشد از فروشنده (مؤ لف) اجازه بگیرد آزادانه آن نسخه را دوباره بفروشد یا اجاره دهد[۱۲].

استفاده از قرارداد حق امتیاز این مزیت را دارد که امکان اجتناب از این نظریه را فراهم می‌آورد به نحوی که کاربر نتواند آزادانه نسخه خاص خود را به دیگران انتقال داده و باعث ایراد ضرر و زیان به فروشنده شود یا آنرا به دیگری، که ممکن است بطور غیر قانونی آنرا تکثیر کند، اجاره دهد.

این نظریه در ماده ۱۰۹ قانون حق مؤلف[۱۳] ایالات متحده آمریکا مصوب ۱۹۷۶ بیان شد. اما از آنجا که شرکت‌هایی تأسیس شدند که کارشان اجاره نرم‌افزار به کاربرانی بود که ممکن بود بصورت غیر قانونی از آن تکثیر کنند، این نظریه در خصوص برنامه‌های کامپیوتری اصلاح شد. (قانون اصلاحیه اجاره نرم‌افزارهای کامپیوتری مصوب ۱۹۹۰) [۱۴] براساس این اصلاحیه، نظریه اولین فروش فقط به کتابخانه‌های غیر انتفاعی و مؤسسات آموزشی اجاره می‌دهد که نسخه‌هایی از نرم‌افزار را اجاره دهند. با این حال هنوز خریدار یک برنامه کامپیوتری دارای حق مؤلف می‌تواند آزادانه آنرا مجدداً به دیگری بفروشد[۱۵].

۴ـ وضع شروط جانبی مثل انتخاب قانون حاکم، شرط داوری، دادگاه صالح، شرط سند واحد[۱۶] و ...

۵ـ تجویز اعمالی که بدون اجازه مؤلف ممکن است قانوناً نقض حق مؤلف بشمار رود مثلاً اجازه داشتن نسخه پشتیبان (back-up)

۶ـ ایجاد خیار فسخ قرارداد حق امتیاز و توسل به طرق جبران خسارت. البته این اضافه بر طرق و راهکارهایی است که قانون حق مؤلف پیش‌بینی کرده است.

۷ـ معطوف ساختن توجه کاربر به حق مالکیت فکری مؤلف و تأکید بر مقررات مربوطه.

۸ـ قادر ساختن مالک نرم‌افزار به فروش خدمات پشتیبانی خود. این خدمات اغلب برای مدت محدودی رایگان و سپس هزینه‌بر است.[۱۷]

۹ـ تحمیل محدودیت‌ها و استثنائاتی بر مسئولیت مالک نرم‌افزار: مثلاً نرم‌افزاری که ۲۰۰ دلار بیشتر نمی‌ارزد نمی‌تواند خسارت غیر مستقیم بیش از قیمت خودش ببار آورد. در حقوق انگلستان مسئولیت کالا براساس ماده ۷ قانون حمایت از مصرف کننده مصوب ۱۹۸۷ [۱۸] قابل سلب شدن نیست[۱۹].

۱۰ـ روشن ساختن ضمانت‌هایی (Warranties) که مالک نرم‌افزار می‌نماید و ضمانت‌هایی که از خود سلب می‌کند. در حقوق انگلستان براساس قانون فروش کالا ۱۹۷۹ [۲۰] و در حقوق ایالات متحده براساس قانون متحدالشکل تجاری[۲۱] بطور ضمنی ضمانت‌هایی به عهده دارد که می‌تواند براساس قانون از خود سلب کند. مهم‌ترین ضمانت وی این است که نرم‌افزار مطابق توصیف مندرج در دفترچه راهنما عمل کند. (performance warranty)

۱۱ـ تعهد به رازداری: کاربر موظف است اسرار مربوط به نرم‌افزار را حفظ کند. بنظر می‌رسد این تکلیف در خصوص نرم‌افزارهایی که در سطح گسترده در اختیار عموم قرار می‌گیرد عملی نباشد[۲۲].

۱۲ـ محدود کردن روش استفاده از نرم‌افزار: مثلاً کاربر موظف است نرم‌افزار را به مقاصد داخلی استفاده کند نه به قصد خدمات‌رسانی به دیگر شرکت‌ها. محدودیت دیگر مربوط به کامپیوتر می‌شود به این معنی که کاربر فقط می‌تواند نرم‌افزار را بر روی یک کامپیوتر نصب کند. این محدودیت به شرط «یک نسخه روی یک واحد پردازش کننده مرکزی (سی‌پی‌یو) در آن واحد[۲۳]» معروف است.

این شرط در بیان ساده به این معنی است که همانطور که شما زمانی که یک کتاب می‌خرید و حق استفاده از آنرا پیدا می‌کنید ـ نه حق تکثیر آنرا ـ اگر بخواهید در منزل استفاده کنید با خود به منزل می‌برید و اگر بخواهید در اداره استفاده کنید با خود به اداره می‌برید ... در مورد نرم‌افزار ـ که تکثیر آن ساده‌تر است هم همینطور است می‌گویند روی یک CPU می‌توانید کپی کنید هر جایی بخواهید استفاده کنید چه منزل چه اداره باید با خود ببرید.

در موردی که نرم‌افزاری روی یک پایانه (terminal) نصب شده و چند کامپیوتر با یک سرور (server) به هم متصل شده‌اند سؤال شده آیا کاربر کامپیوتری که نرم‌افزار روی آن نصب نشده می‌تواند از آن استفاده کند؟ در جواب می‌گوییم بله مشروط به اینکه در همان لحظه کاربر دیگری از آن نرم‌افزار استفاده نکند. البته اگر کسی بگوید در اینجا CPU سرور هم حساب است و در آن واحد دو CPU به نرم‌افزار دسترس دارند دچار مشکل می‌شویم[۲۴].

این قاعده در قانون ما به نحو دیگری مورد پذیرش قرار گرفته است. ماده ۷ قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای مقرر می‌دارد: «تهیه نسخه‌های پشتیبان و همچنین تکثیر نرم‌افزاری که بطریق مجاز برای استفاده شخصی تهیه شده است، چنانچه بطور همزمان مورد استفاده قرار نگیرد بلامانع است.»

بر این اساس کاربر می‌تواند براحتی از نرم‌افزاری که بطریق مجاز تهیه شده نسخه‌های دیگری تهیه کند و روی چند CPU نصب کند مشروط بر اینکه به‌طور همزمان مورد استفاده قرار نگیرند: یعنی در آن واحد بیش از یکی از نسخه‌ها مورد استفاده قرار نگیرند. با توجه به آمره بودن ماده مذکور بنظر می‌رسد شرط خلاف آن هم نافذ نباشد.

هدف از شرط «یک نسخه روی یک سی‌پی‌یو در زمان واحد» تنظیم درآمد تولید کننده و پرداخت مناسب در قبال استفاده از نسخه مذکور می‌باشد. بدیهی است تنها در زمانی این شرط در قرارداد شرینک رپ ضروری است که قانون چنین محدودیتی را وضع نکرده باشد.

هدف دوم (تضمین حقوق مالکیت فکری مؤلف) در حال حاضر، در حقوق کنونی، بیشتر جنبه تاریخی دارد و مربوط به زمانی است که هنوز قوانین حق مؤلف (Copy right) و حق اختراع وضع نشده بود و حمایت قانونی از آثار فکری وجود نداشت. در چنین شرایطی مؤلفین سعی می‌کردند با بستن عقد مستقلی با استفاده کننده او را ملزم به رعایت حق مالکیت فکری خود سازند. در کشور ما نیز اگر چه در قوانین حق مؤلف پدید آورنده نرم‌افزار برسمیت شناخته شده ولی هنوز فقهایی هستند که حق مؤلف

را حقی نامشروع می‌پندارند. این افراد تأکید کرده‌اند با این حال قرار دادن مفاد حق مؤلف در چهارچوب قراردادی بلامانع و الزام‌اور است[۲۶].

هدف اول (اعطای امتیاز بهره‌برداری به کاربر) هم بنفسه با توجه به آنچه گفتیم لغو و بی‌فایده است. چرا که در حال حاضر قانون حق مؤلف بنفسه این حق را به کاربری که از طریق مجاز نسخه نرم‌افزاری را تهیه کرده می‌دهد که بدون اینکه نیاز باشد از مؤلف اجازه بگیرد از نسخه خود استفاده کند. این مسأله از ماده ۷ قانون حمایت از پدیدآورندگان نرم‌افزارهای رایانه‌ای قابل استنباط است.

آنچه در بندهای سه، شش، نه، ده، یازده و دوازده آمده را می‌توان بطور کلی تحت عنوان هدف «محدود کردن حقوق کاربر» جای داد. بیشتر نویسندگان معتقدند که هدف اساسی از قرارداد شرینک رپ همین هدف است. بررسی این هدف احتیاج به تحلیل دقیق‌تری دارد اصولاً یکی از استدلالاتی که مخالفین اعتبار این قرارداد بیان می‌نمایند همین است که قرارداد شرینک رپ بعنوان روشی برای اعمال زور، فشار و تحمیل شروط اجباری به خریدار و کاربر بکار می‌رود[۲۸].

تقریباً همه صاحبنظران معتقدند که براساس قانون حق مؤلف، بهره‌برداری از نسخه نرم‌افزاری برای کاربر مجاز، مشروع است. لذا محدود کردن چنین حق بهره‌برداری مشروع غیر معقول (on reasonable) است[۲۹].

با این حال، بنظر می‌رسد این دیدگاه با نگاهی جامع بایستی تحلیل شود و در این راستا به حمایت فعلی قانون از اثر فکری نرم‌افزار و حمایتی که لازم است قانون از آن بنماید توجه شود.

ابتدا این نکته لازم به ذکر است که اگر محدود کردن کاربر در شکل محدود کردن به کامپیوتر یا به عبارت دیگر قاعده «یک نسخه روی یک CPU در زمان واحد» باشد همانطور که قبلاً اشاره کردیم اشکالی در مشروعیت آن بچشم نمی‌خورد و مردود دانستن این قاعده به معنی بهم خوردن نظام مالی تولید کننده نرم‌افزار است چرا که در این صورت فردی با پرداخت مبلغی معادل مبلغ حق امتیاز استفاده شخصی آنرا به شکلی در مؤسسه‌ای که در آن چندین رایانه از طریق سرور بصورت شبکه به هم متصل شده‌اند در اختیار کاربران متعدد قرار می‌دهد که می‌توانند در آن واحد به آن دسترسی داشته باشند که مصداق دارا شدن غیر عادلانه واکل مال بباطل می‌باشد.

انگیزه تولید کنندگان از محدود کردن کاربر ممکن است علاوه بر مطلب فوق

۱) جلوگیری از فروش یا هر نوع انتقال آن نسخه به دیگری
۲) جلوگیری از تکثیر، اصلاح، ترجمه یا تغییر برنامه توسط کاربر
۳) جلوگیری از تجزیه (decompiling) توسط کاربر

باشد. این هر سه با یکدیگر ارتباط متقابل دارند و مبنای همگی آنها جلوگیری از مهندسی معکوس (Reverse engineering) است[۳۰].

تولیدکنندگان نرم‌افزار مبالغ زیادی صرف اطلاعات نرم‌افزار کرده‌اند و حاصل آن تولید الگوریتم (algoritm) نرم‌افزار می‌باشد. الگوریتم ویژگی حیاتی نرم‌افزار است که عملکرد آن کاملاً وابسته به همین الگوریتم است. به عبارت دیگر تولید کنندگان نسبت به الگوریتم‌های ایجاد شده حقوق مالکانه‌ای پیدا کرده‌اند. لذا است که از سرقت حقوق خود به وسیله مهندس معکوس و کشف الگوریتم بیم دارند. بهمین خاطر است که درصدد آن هستند که مبنای قراردادی برای آن ایجاد کنند و با ممنوع کردن مهندسی معکوس حقوق مالکانه خود را حفظ کنند.

اما آیا حمایت قانونی از نرم‌افزار کافی برای حمایت از الگوریتم آن نیست؟ به عبارت دیگر با حمایت قانونی از الگوریتم توسط قوانین حق مؤلف و حق اختراع و نتیجتاً ممنوعیت مهندسی معکوس آیا دیگر جایی برای حمایت قراردادی باقی خواهد ماند؟ در جواب باید گفت زمینه اولیه این سؤال نادرست است. قانونگذار از الگوریتم، بنفسه، حمایت قانونی نکرده است. قانونگذار زمانی از اثر حمایت می‌کند که ویژگی‌های حق مؤلف یا حق اختراع را داشته باشد. در حالی که الگوریتم بنفسه ابداع و اختراع محسوب نمی‌شود تا حق اختراع به آن تعلق گیرد و خصوصیات و ویژگی‌های آن به نحوی است که مشمول حق مؤلف هم نمی‌شود. یا اگر صراحتاً این مطلب را نگوییم باید گفت که وضعیتی مبهم دارد. به همین خاطر که دیوان عالی در پرونده لوتوس Lotus حاضر نشد به این مسأله بپردازد و جواب سؤال فوق را بدهد[۳۱].

این در حالی است که باید بین حمایت قانونی از اثر و آشکارسازی اثر توسط مؤلف تعادل برقرار باشد. هر قدر حمایت قانونی از اثر بیشتر باشد مؤلف تمایل بیشتری به خلق اثر و آشکارسازی آن دارد و هر چه کمتر باشد وی ترجیح می‌دهد که اثر خود را مخفی سازد تا مورد سوء استفاده قرار گیرد. همانطور که گفتیم قانونگذار حمایت مناسبی از الگوریتم ارائه نداده است لذا تولید کنندگان نرم‌افزار سعی می‌کنند با استفاده از قراردادهای حق امتیاز این خلاء را پر نمایند.

با توجه به این وضعیت آیا بهتر نیست مهندسی معکوس توسط قانونگذار ممنوع گردد؟

در پاسخ به این سؤال می‌گوییم مهندسی معکوس ممکن است به یکی از این دو هدف انجام شود:

۱) شناسایی سازگاری نرم‌افزار با دیگر نرم‌افزار یا سخت‌افزار.

۲) شناسایی الگوریتم نرم‌افزار.

از این دو هدف هدف اولی کاملاً مشروع و عقلایی است و جلوگیری از آن جلوی رقابت را می‌گیرد. اما دومی خیر هدفی است نامشروع که ممنوع کردن آن مانع رقابت تولید کنندگان هم نمی‌شود. (این تفکیک در دستورالعمل‌های شورای اروپا نیز دیده می‌شود[۳۲])

بنابراین مهندسی معکوس بنفسه عمل نامشروعی نیست بلکه بستگی به هدف فاعل آن دارد اگر بقصد شناسایی سازگاری باشد مشروع و اگر به قصد کشف الگوریتم و سوء استفاده از آن باشد عملی نامشروع است.

رویه قضائی ایالات متحده هم مؤید این نتیجه‌گیری است. در ایالات متحده ۳ پرونده در این خصوص وجود دارد: پرونده sega، پرونده nintendo و در رأس آنها پرونده vaulto. نقطه مشترک این هر سه، مشروعیت مهندسی معکوس به قصد شناسایی سازگاری می‌باشد[۳۳].

بنابراین مشروعیت مهندسی مذکور مستلزم این است که حمایت قانونی مناسبی از الگوریتم بنحو روشنی با حدود و صغور مشخصی ایجاد شود. در حال حاضر با توجه به فقدان چنین حمایتی استفاده از قرارداد حق امتیاز و محدود کردن کاربر عمل عقلایی است و نباید به دلیل لطمه زدن به حقوق کاربر آنرا بی‌اعتبار تلقی کرد. منتها شرط قراردادی که مهندسی معکوس بقصد شناسایی سازگاری را ممنوع سازد شرطی باطل و خلاف نظم عمومی شمرده می‌شود[۳۴].

مبحث سوم: اعتبار قرارداد حق امتیاز شرینک رپ

مسأله اعتبار (enforceability) قراردادهای سه‌گانه شرینک رپ، کلیک‌رپ و بروز رپ مهم‌ترین مسأله‌ای است که در مورد این قراردادها به چشم می‌خورد و سایر مباحث همگی دایر مدار اعتبار یا عدم اعتبار این قرارداد می‌باشند. منظور ما از اعتبار نفوذ و صحت آن است یعنی آیا چنین قراردادی قانوناً صحیح و واجد آثار حقوقی است یا اینکه به علت اشکالات اساسی که در آن به چشم می‌خورد باطل و بلااثر می‌باشد. مسأله اعتبار قرارداد شرینک رپ آنقدر حائز اهمیت است که بسادگی دادگاه‌ها، وکلا و دانشجویان حقوق را به دو گروه تقسیم کرده است: گروهی آنرا قراردادی صحیح و نافذ در معاملات کالاهای انبوه که طرفین به صورت حضوری معامله نمی‌کنند آنرا اجتناب‌ناپذیر قلمداد می‌کنند: گروه دیگر با توسل به اصول سنتی حاکم بر قراردادها آن را باطل و بدون اثر حقوقی دانسته و آنرا وسیله‌ای برای اعمال فشار و تحمیل شروط اجباری به خریدار و کاربر قلمداد می‌کنند.
دادگاه‌ها کراراً رأی بر بطلان این قرارداد داده‌اند.
پرونده‌های Arizona Retail system و Step-saver ، Knocek V.gateway همگی پرونده‌هایی هستند که در آن دادگاه اعتبار این قرارداد را رد کرده و آنرا الزام‌آور ندانستند.

۱ـ اشکالات وارده

اشکالات وارد بر این قرارداد را در آخر مبحث معرفی ذکر کردیم. از این میان چند اشکال در مبحث فواید مطرح شد و باقی را در همین جا مطرح خواهیم کرد. مهم‌ترین اشکالی که محور توجه دادگاه‌ها بوده اولین اشکال یعنی اشکال عدم اطلاع خریدار محصول هنگام انعقاد بیع می‌باشد: چگونه ممکن است فردی ملزم به چیزی شود که هنگام اعلام قبولی عقد از آن اطلاع نداشته است؟ این اشکال اساس و محوری‌ترین اشکال وارده است که تقریباً در هر سه نوع قرارداد مذکور به نوعی به چشم می‌خورد. بیشتر نویسندگان در مقام بحث از اعتبار این قرارداد فقط از همین اشکال نام برده‌اند.
ما ابتدا دیگر اشکال‌های وارده که اغلب در رابطه با قرارداد شرینک رپ مطرح شده‌اند را مطرح کرده و سپس در نهایت اشکال اساسی را بیان کرده و به مسأله اعتبار قراردادهای کلیک رپ و بروز رپ هم اشاره می کنیم: ذکر این نکته خالی از فایده نیست که مسأله اعتبار این قرارداد چیزی نیست که در این مجال کوتاه بتوان به آن پاسخ قطعی داد و یقیناً در کشور ما هم موافقان و مخالفانی خواهد داشت:
اولین اشکال: در قرارداد شرینک رپ تولید کننده بعنوان موجب (ایجاب کننده) قرارداد شرینک رپ لزوماً تعیین می‌کند که قبول به روشی خاصی یعنی با پاره کردن نایلون بسته‌بندی یا استفاده از نرم‌افزار بعمل آید؟ اصولاً آیا موجب دارای چنین حقی است که بتواند نحوه قبول را تعیین کند؟ با توجه به اینکه اساس عقد همکاری ارائه طرفین است و با اعلام قبول این همکاری محقق می‌شود و با توجه به اصل رضایی بودن قراردادها چنانچه قابل به نحو دیگری قبول خود را به اطلاع موجب برساند آیا عقد واقع نمی‌شود؟
آنچه چه در حقوق کامن‌لا چه در حقوق رومی ژرمنی قابل دفاع است این است که چنانچه موجب روش خاصی را برای اعلام قبول تعیین کرده باشد تبعیت از این روش لازم است. در حقوق کامن‌لا این قاعده در پرونده اِلیاسون علیه هنشا و (Eliason V.Henshaw) سال ۱۸۱۹ وضع شد[۳۵]. در حقوق رومی ژرمنی هم می‌توان همین نتیجه را پذیرفت چرا که از شروط قبول آن

است که قابل ایجاب را به همان نحوی که هست بپذیرد و پذیرش ایجاب به روش غیر از روش تعیین شده در خود ایجاب، قبول بدون قید و شرط محسوب نمی‌شود. در حقوق ما هم از آنجا که براساس مواد ۱۹۱ و ۱۹۳ قانون مدنی اعلام اراده به وسیله‌ای غیر از لفظ جایز است و با توجه به لزوم مطابقت ایجاب و قبول ماده ۱۹۴ قانون مدنی همین راه‌حل پذیرفتنی است.

اشکال دوم: در حقوق کامن لا قاعده این است که شرط نفوذ عقد آن است که قبول به اطلاع موجب برسد. یعنی قابل بایستی اراده خود را مبنی بر پذیرش مفاد ایجاب به اطلاع موجب برساند. با این حال در قرارداد شرینک رپ که اعلام رضایت کاربر به مفاد قرارداد حق امتیاز با پاره کردن نایلون بسته‌بندی یا استفاده از نرم‌افزار بعمل می‌آید هیچ‌گاه به اطلاع موجب نمی‌رسد. از بند ۲ ماده ۱۸ و ماده ۲۳ کنوانسیون سازمان ملل راجع‌به قراردادهای بیع بین‌المللی کالا هم استفاده می‌شود که عقد در زمان وصول قبول به ایجاب‌کننده منعقد می‌شود: بند ۲ ماده ۱۸ اشعار می‌دارد: «قبول ایجاب زمانی مؤثر می‌شود که رضایت قبول کننده به اطلاع موجب برسد.»

ماده ۲۳: « قرارداد زمانی منعقد می‌شود که قبول براساس مقررات این کنوانسیون مؤثر شود[۳۶] »

فارق از بحثهای مربوط به حقوق خارجی، بنظر می‌رسد در حقوق ایران تکلیف این مسأله روشن باشد. در حقوق ایران وصول قبول به ایجاب کننده شرط تحقق عقد شمرده نمی‌شود: اولاً شرط لازم برای تشکیل عقد، علی‌الاصول، تحقق همکاری دو اراده است و همکاری دو اراده با اعلام قبول توسط قبول کننده محقق می‌شود. ثانیاً ماده ۱۹۱ قانون مدنی اشعار می‌دارد: «عقد محقق می‌شود به قصد انشاء به شرط مقرون بودن به چیزی که دلالت بر قصد کند.» در این ماده برای تحقق عقد اعلام قبول کافی می‌باشد و لزومی به وصول قبول به ایجاب کننده نمی‌باشد لذا در عقود مکاتبه‌ای عقد در زمان اعلام و ارسال قبول محقق می‌شود نه زمان وصول قبول[۳۷].

اشکال سوم: در حقوق کامن‌لا هر قراردادی بایستی عوض "consideration" داشته باشد عوض رکن هر قراردادی محسوب می‌شود مثلاً عوض انتقال مبیع برای بایع پرداخت ثمن توسط مشتری است و عوض تعهد به پرداخت ثمن توسط مشتری، انتقال مالکیت مبیع به مشتری می‌باشد. در حقوق کامن لا قرارداد بدون عوض یا به عبارت دیگر تعهد «خشک و خالی» نافذ نیست[۳۸]. در قرارداد شرینک رپ اشکال شده که این قرارداد از جانب کاربر فاقد عوض است؛ امتیاز دهنده (licensor) در ازاء این قرارداد عوضی که دریافت می‌کند همانا ایجاد محدودیت‌ها و الزاماتی بر کاربر در خصوص نحوه استفاده از نرم‌افزار است اما کاربر در ازاء این تعهدات چه عوضی دریافت می‌نماید؟ به عبارت دیگر در این قرارداد معمولاً امتیاز دهنده هیچ‌گونه تعهدی را بعهده نمی‌گیرد بلکه ضمانت‌ها و مسئولیت‌های خود را سلب می‌کند. برای گریز از این اشکال است که امتیازدهنده سعی می‌کند در این قرارداد تعهدی هر چند ناچیز به عهده بگیرد و این تعهد اغلب در قالب ضمانت (warranty) خاصی جلوه می‌کند. در جواب به این اشکال گفته شده که عوضی که کاربر دریافت می‌کند امتیاز بهره‌برداری از نرم‌افزار است. این پاسخ پاسخ مناسبی به شمار نمی‌رود چرا که همانطور که سابقاً اشاره کردیم امتیاز بهره‌برداری چیزی نیست که هدیه امتیازدهنده به امتیاز گیرنده (Licensee) باشد بلکه اجازه‌ای است که بوسیله قانون به کاربر مجاز اعطا شده است.

در حقوق رومی ژرمنی نظریه عوض "consideration" پذیرفته نشده بلکه بجای آن نظریه جهت قرارداد (La Cause du contrat) پذیرفته شده است.

اشکال چهارم: اشکال تحمیلی بودن شروط قرارداد شرینک رپ می‌باشد: این قرارداد شکل یک قرارداد نمونه و فرم از قبل توسط تولید کننده نرم‌افزار تهیه شده و بدین وسیله محدودیت‌ها و تکالیف بسیاری بر کاربر بار کرده است. شروطی که عمدتاً به ضرر کاربر می‌باشد. قدرت اقتصادی بالای تولیدکنندگان انبوه محصولات فروش انبوه Mass Market تعادل اختصاری و اطلاعاتی بین طرفین عقد را بر هم می‌زند به شکلی که کاربر اصلاً امکان چانه زنی در مورد شروط قرارداد را ندارد او می‌تواند قبول کند یا قبول نکند این تنها گزینه پیش روی کاربر است.

این اشکال که در واقع در مورد کلیهٔ قراردادهای نمونه (Standard form) مطرح شده بلحاظ خاصیت تحمیلی یا الحاقی بودن آنها است. به عقدی الحاقی یا تحمیلی می‌گویند که بلحاظ عدم تعادل اختصاری طرفین عمده مفاد قرارداد به ضرر یک طرف آن باشد و وی در عمل چاره‌ای جز پذیرفتن آن ندارد.

برای رفع این اشکال هم قانونگذار دخالت کرده و هم دادگاه‌ها. قانونگذار با تصویب قانون‌هایی از مشتری حمایت می‌کند و شروط ناروا را باطل اعلام می‌نماید در آمریکا قانون شروط قراردادی ناروا مصوب ۱۹۷۷ [۴۰] و در انگلستان قانون حمایت از مصرف‌کننده[۴۱] مصوب ۱۹۸۷ همین وظیفه را به عهده دارند و شروطی را که غیرمعقول[۴۲] تشخیص داده شود غیر نافذ می‌شمارند. از طرف دیگر دادگاه‌ها در قالب تفسیر قضائی به کمک طرف ضعیف آمده و سعی می‌کنند قرارداد را به نحوی تفسیر کنند که از بار تحمیلی آن برطرف ضعیف کاسته شود[۴۳].

اشکال پنجم: این اشکال در حقیقت مربوط به ماهیت حقوقی قرارداد تهیه نرم‌افزار می‌شود از یک طرف بین خریدار (کاربر) با فروشنده (توزیع کننده) بروشنی یک عقد بیع دیده می‌شود که بدان وسیله مالکیت یک نسخه از نرم‌افزار موجود دربسته نرم‌افزاری به مشتری منتقل می‌شود و کاربر پس از آن متوجه قرارداد حق امتیازی می‌شود که در آن ذکر شده قرارداد بین مالک نرم‌افزار (نویسنده نرم‌افزار) و کاربر نهایی منعقد می‌شود.

درباره ماهیت این رابطه حقوقی احتمالات مختلفی داده شده است[۴۴]. در حقوق کامن‌لا این بحث بعنوان اشکال وارد براصل نسبی بودن[۴۵] قراردادها مطرح شده است. به این معنی که عقد ماهیتاً با توجه به قصد و اراده طرفین عقد بیع است و طرفین آن کاربر و توزیع کننده هستند و کلیه شروط حق امتیاز تعهد به نفع شخص ثالث (نویسنده نرم‌افزار) هستند که از طرف توزیع‌کننده بر کاربر در حین عقد تحمیل می‌شوند و برای وی لازم‌الاجرا می‌باشند[۴۶].

قاضی پرونده Beta V.Adobe سال ۱۹۹۶ رأی داد که فقط یک قرارداد بین ۳ طرف وجود دارد. یک طرف قرارداد می‌تواند حقوقی بنفع شخص ثالث (نویسنده نرم‌افزار) ایجاد کنند این حقوق بین شخص ثالث و کاربر نهایی لازم‌الاتباع هستند و در عین حال جزئی از قرارداد بین کاربر نهایی و توزیع‌کننده هم هستند[۴۷].

در حقوق انگلستان مفهوم تعهد به نفع ثالث با تصویب قانون عقود (حقوق اشخاص ثالث) مصوب ۱۹۹۹ [۴۸] پذیرفته شد. مع‌الوصف برای اینکه در قرارداد حقوق شخص ثالث هم مرعی باشد بایستی صراحتاً به قانون ۱۹۹۹ اشاره کرده باشد[۴۹].

اشکال اساسی: عدم اطلاع مشتری از مفاد قرارداد حق امتیاز هنگام قبول: این اشکال اساسی‌ترین و گاه تنها اشکالی است که مورد توجه صاحبنظران قرار گرفته است و آراء متعدد دادگاه‌ها مبتنی بر عدم اعتبار قرارداد شرینک رپ بر همین مبنا بوده است. از آنجا که مشتری بواقع بشروط قرارداد حق امتیاز رضایت نمی‌دهد لذا این شروط جزء قرارداد بیع به حساب نمی‌آیند. به عبارت دیگر بر مبنای نظریه «حاکمیت اراده[۵۰]» در سیستم رومن ژرمنی و نظریه «مذاکره[۵۱]» در سیستم کامن لا تنها زمانی یک قرارداد شکل می‌گیرد که طرفین از وجود و محتوای چنین قراردادی آگاه باشند و با چنین آگاهی نسبت به قرارداد تراضی

کنند[۵۲]. این عنصر یعنی عنصر آگاهی در قرارداد شرینک رپ نیست چرا که قبول کننده از مفاد ایجاب آگاهی ندارد. لذا تطابق بین ایجاب و قبول که شرط ایجاد تراضی و درنتیجه عقد می باشد وجود ندارد[۵۳].

قاضی هلرستین Hellerstein در مقام بیان این قاعده اظهار می‌دارد «تعهدات زمانی الزام‌آور می‌شوند که تلاقی اراده‌ها و تبادل عوضین انجام شود. این قاعده بمدت دو قرن است که در کامن‌لا وجود دارد و الان هم به همان قوت وجود دارد.»

طرفداران اعتبار قرارداد شرینک رپ در مواجهه با این اشکال پاسخ‌های متفاوتی داده‌اند:

گفته شده که همینکه مشتری می‌داند که استفاده از نرم‌افزار مشروط به رعایت کردن قرارداد حق امتیاز است و وی این هشدار را روی بسته نرم‌افزاری می‌بیند برای قبول قرارداد و انعقاد آن کافی است اینکه می‌گویند رضایت «واقعی» شرط است نادرست است. حقوق در زمان ایجاد راه‌آهن و اختراع تلگراف هیچ‌گاه رضایت «واقعی» را شرط ندانسته است. حقوق قرارداها هم نمی‌تواند چنین شرطی بگذارد. تولیدکنندگان بزرگ نمی‌توانند با مشتریانشان سر میز گفتگو بر سر شروط قرارداد حق امتیاز بنشینند[۵۴].

دلیل دیگری که طرفداران اعتبار قرارداد شرینک رپ می‌آورند وحدت ملاک و مشابهت با قراردادهای نمونه است. قرارداد نمونه فرم چاپی است که توسط یکی از طرفین قرارداد تهیه شده و طرف دیگر بدون امکان چانه‌زنی درباره شروط قراردادی یا با امکان کم نسبت به آن رضایت می‌دهد.

امروزه این قراردادها در کلیه معاملات چه تجاری چه شخصی مرسوم و رایج شده‌اند. و در معاملات انبوه استفاده از این قرارداد گریزناپذیر است. مفهوم قراردادهای نمونه اولین بار توسط پروفسور اِل ریزر(Prof. L. Raiser) در آلمان سال ۱۹۳۵ مطرح شد[۵۵].

این قراردادها مورد قبول قرار گرفته‌اند قاعده کلی این است که شروط قراردادهای نمونه همگی معتبرند مگر آنها که نامتعارف و غیر معقول هستند. قانون حمایت از مصرف کننده در انگلستان بر این مطلب تأکید دارد.

پروفسور کاواکامی بر مبنای نظریاتی از آلمان و ژاپن قاعده‌ای را پیشنهاد می‌کند: از آنجا که اشکال عدم اطلاع از شروط، اغلب در شروط غیر اساسی عقد نمونه مطرح شده‌اند بایستی بین شروط اساسی و غیر اساسی تفکیک کرد شروط اساسی بایستی به اطلاع طرفین برسد اما شروط غیر اساسی تنها در دو صورت بایستی پذیرفته شوند:

۱) قبل از پذیرش شروط اساسی، شروط غیر اساسی به نحوی در دسترس طرف عقد قرار گیرند که وی «امکان و فرصتی معقول» جهت بررسی آنها داشته باشد.

۲) شروط غیر اساسی در تعارض با شروط اساسی یا شروطی که به روشنی بر سر آنها مذاکره شده است نباشد[۵۶].

طرفداران نظریه اعتبار قرارداد شرینک رپ استدلال می‌کنند که قرارداد شرینک رپ اگر یک قرارداد نمونه نباشد، از این حیث با این نوع قراردادها حکم یکسانی دارد لذا همانطوری که قرارداد نمونه قانوناً معتبر است این قرارداد هم بایستی معتبر دانسته شود[۵۷].

آخرین استدلالاتی که بر صحت و اعتبار قرارداد شرینک رپ شده است این است که اطلاع از شروط قرارداد اینطور نیست که لزوماً باید قبل از پرداخت ثمن معامله باشد. در مورد قراردادهای بیمه و قرارداد خرید بلیط هواپیما این معاملات

مرسوم است که ابتدا مشتری پرداخت می‌کند سپس شروط قرارداد را می‌بیند قاضی فرانک استِربروک قرارداد شرینک رپ را بسادگی از نوع قراردادهای «الان بپرداز بعداً شروط را ببین[۵۸]» می‌شمارد[۵۹].

بر این مبنا انعقاد قرارداد تا زمان رؤیت شروط توسط کاربر و رضایت به آن عقب می‌افتد و پس از آن اگر کاربر رضایت داد که عقد الزام‌آور می‌شود و اگر رضایت نداد می‌تواند با استرداد نسخه نرم‌افزار پول پرداختی خود را پس بگیرد. این استدلال مورد توجه قانونگذار و رویه قضایی ایالات متحده واقع شده است.

۲ـ رویه قضایی ایالات متحده

در حقیقت می‌توان گفت که رویه دادگاه‌ها در خصوص قرارداد شرینک رپ دو مرحله دارد: رویه قدیم که مبتنی بر عدم نفوذ قرارداد شرینک رپ بود این رویه در پرونده‌های Step-saver systems Inc V. wyse technology سال ۱۹۹۱، Arizona Retail Systems Inc. V Software Link Inc ، Vault Corp. V. Quaid Software Ltd متجلی شد این سه پرونده همگی قبل از پرونده ProCD بود که با این پرونده رویه قضائی وارد مرحله جدیدی شد. در این پرونده دادگاه بدوی رأی بر عدم اعتبار قرارداد شرینک رپ داد اما این رأی در تجدیدنظر نقض شد و دادگاه تجدیدنظر قرارداد شرینک رپ را قراردادی صحیح و معتبر تلقی کرد. بعد از این دادگاه‌ها در پرونده‌های ذیل از منطق و استدلال پرونده ProCD تبعیت کردند.

1- Lan Systems Inc V. Netscout service Level Corp. 2007
2- Hill V. Gateway 2000
3- Mortenson V. Timberline 1999
4- Brower V. Gateway 2000 Inc 1998

با این حال قاضی پرونده Klocek V. Gateway 2000 استدلال قاضی پرونده ProCD را نپذیرفت و رأی بر عدم اعتبار قرارداد شرینک رپ داد[۶۰].

برای آشنایی با استدلالات دادگاه‌ها بهترین پرونده، پرونده ProCD است. در رأی قاضی دادگاه بدوی می‌توان استدلال مخالفین اعتبار قرارداد شرینک رپ و در رأی قاضی دادگاه تجدیدنظر می‌توان استدلالات و پاسخ موافقین را یافت. لذا در اینجا شرح مختصری از پرونده ارائه می‌کنیم.

گزارش پرونده ProCD, Inc V. Zeidenberg

شرکت ProCD با صرف میلیون‌ها دلار یک لیست تلفن شخصی و تجاری جامع تهیه کرد سپس آنرا به صورت اطلاعات دیجیتال همراه نرم‌افزاری که امکان دسترسی به این اطلاعات را فراهم می‌کرد داخل یک سی‌دی‌رام باسم تجاری Select Phone TM به بازار عرضه کرد. در روی بسته سی‌دی‌رام بطور مختصر و با حروف ریز چنین نوشته شده بود: «استفاده کاربر از دیسکت و لیست اطلاعات به معنی رضایت به شروط قرارداد حق امتیاز است. در این صورت وی ملزم به رعایت شروط قرارداد است.»

متهم مَتِو زیدنبرگ (Mathew Zeidenberg) پس از خرید نسخه اولیه و نسخه بروز شده این دیسکت شرکتی به نام Silken Moutain تأسیس کرد و با استفاده از این دیسکت و دیسکت مشابهی از شرکتی دیگر، از طریق اینترنت به فروش خدماتی در همین رابطه پرداخت. این شرکت به تصور عدم اعتبار قرارداد شرینک رپ نام تجاری سازنده را هم حذف کرده بود.

شرکت ProCD علیه زیدنبرگ و شرکت وی Silken بدلیل نقض حق مؤلف و قرارداد حق امتیاز شکایت کرد[۶۱].

رأی دادگاه بدوی

دادگاه ادعای نقض حق مؤلف را رد کرد چرا که دیسکت مذکور مشمول حمایت قانونی حق مؤلف نمی‌شود و بیشتر از آنکه یک اثر فکری باشد یک سری اطلاعات با ارزش شمرده می‌شود.

در خصوص ادعای تخلف از قرارداد حق امتیاز: دادگاه ابتدا روشن کرد که ماهیت عمل حقوقی انجام شده عقد بیع است نه قرارداد حق امتیاز لذا بایستی در چهارچوب قانون یکنواخت تجاری، پرونده حل و فصل شود، چون اگر حق امتیاز بود پرداخت به صورت یکجا بود نه قسطی؛ اگر حق امتیاز بود شرکت نرم‌افزاری مالکیت آن نسخه را برای خود حفظ می‌کرد نه اینکه منتقل کند به مشتری؛ و اگر حق امتیاز بود حداکثر مدت امتیاز مشخص می‌شد در حالی که در اینجا هیچ زمانی برای انقضای حق امتیاز پیش‌بینی نشده است.

دادگاه بیان کرد:

«صرف اشاره به اینکه نرم‌افزار مشروط به قرارداد حق امتیاز است امکان مناسبی در اختیار خریدار نمی‌گذارد تا در مورد قبول یا عدم قبول این شروط تصمیم بگیرد. خریدار باید این امکان را داشته باشد که همه شروط را بخواند و بررسی کند. این امکان تنها زمانی محقق می‌شود که خریدار بسته‌بندی نرم‌افزار را باز کند.»

دادگاه اضافه کرد: «گذاشتن بسته نرم‌افزاری در مغازه یک ایجاب است و پذیرش آن توسط مشتری با پرداخت پول یک قبول به شمار می‌رود. مجموع این دو عقد بیع را تشکیل می‌دهند. شروط قرارداد شرینک رپ جزئی از ایجاب نبوده تا داخل در مفاد تراضی طرفین شوند چرا که در زمان فروش به اطلاع مشتری نرسیده و صرف نوشته روی بسته‌بندی هم کفایت نمی‌کند.[۶۲]»

رأی دادگاه تجدیدنظر

دادگاه تجدیدنظر ناحیه هفدهم رأی دادگاه بدوی را در خصوص اعتبار قرارداد شرینک رپ نقض کرد.

دادگاه ناحیه هفدهم تأکید کرد: ادعای دادگاه بدوی در مورد اینکه اطلاع از شروط قرارداد لزوماً باید قبل از پرداخت ثمن معامله باشد مردود است در موارد دیگری هم مشابه این مورد را می‌بینیم که ابتدا پرداخت می‌شود بعد شروط قرارداد را می‌بینیم مثل خرید بلیط هواپیما و بلیط کنسرت موسیقی یا زمانی که شما یک رادیو می‌خرید در زمان خرید از ضمانت‌های بایع اطلاع ندارید و این ضمانت‌ها تنها پس از باز کردن جعبه آشکار می‌شوند.

دادگاه در ادامه اظهار داشت: « اینکه تولیدکنندگان را ملزم کنیم کلیه شروط قرارداد را روی بسته بنویسند بدلیل مفصل بودن شروط و اقتضائات تجاری، اصولاً عملی نیست. ضمناً در برخی موارد اصلاً بسته‌بندی هم وجود ندارد که بتوان شروط را روی آن درج کرد مثل خرید تلفنی.»

دادگاه به بند یک ماده ۲-۲۰۴ قانون یکنواخت تجاری استناد کرد. این ماده اظهار می‌دارد: « قراردادهای فروش کالا ممکن است به هر روشی که برای نشان دادن تراضی کافی باشد بسته شود من جمله رفتار متعاملین.» در این قرارداد ایجاب کننده نحوه قبول را مشخص می‌کند و آن فعلی مثل نصب کردن نرم‌افزار و استفاده کردن از آن است. این عمل برای نشان دادن وقوع تراضی کافی شمرده می‌شود.

آقای زیدنبرگ نیز درست همین کار را انجام داد. او زمانی که نرم‌افزار را نصب کرد شروط قرارداد حق امتیاز ابتدا روی صفحه مانیتور نمایش داده شد و برای نصب کامل نرم‌افزار چاره‌ای نداشت جز کلیک بر روی کلمه «قبول دارم» چرا که در غیر این صورت نرم‌افزار به او اجازه نصب کامل را نمی‌داد.

در حقیقت خریدار زمانی کالا را قبول می‌کند که بعد از امکان بررسی ۶۳ از استرداد کالا خودداری می‌کند و اقدام به استفاده می‌نماید. زیدنبرگ با بررسی نرم‌افزار از مفاد قرارداد حق امتیاز آگاه شد و با این حال کالا را مسترد نکرد. براساس قانون یکنواخت تجاری خریدار این شانس را دارد که تصمیم خود را پس از بررسی کامل اعلام کند[۶۴].

در پایان بحث رویه قضایی به عنوان نتیجه‌گیری این نکته را خاطرنشان می‌کنیم که با توجه به آراء مخالف و آراء موافق مذکور در خصوص اعتبار قرارداد شرینک رپ نبایستی رأی ProCD را پایان کار دانست بلکه هنوز رویه قضائی قاطعی در این باره وجود ندارد. باید دید در نهایت کدام گروه از میدان پیروز بیرون می‌آیند: قائلین به اعتبار یا قائلین به عدم اعتبار.

۳ـ قانون یکنواخت معاملات اطلاعات رایانه‌ای[۶۵]

این قانون قانون جدیدی در ایالات متحده است که بزودی در سراسر جهان تأثیرش آشکار خواهد شد. این قانون (UCITA) حمایت چشمگیری از مالکین نرم‌افزار بعمل می‌آورد. با توجه به اینکه بیشتر نرم‌افزارها یا متعلق به شرکت‌هایی هستند که در ایالات متحده ساکن هستند یا امتیاز بهره‌برداری از آن متعلق به این شرکت‌ها است؛ این قانون ممکن است شرایط قرارداد حق امتیاز را در سراسر جهان تغییر دهد.

این قانون امتیازاتی در اختیار مالک نرم‌افزار قرار می‌دهد: من جمله:

۱) امکان سلب کلیه ضمانت‌های ضمنی که قانون برقرار کرده است.

۲) حق مالک نرم‌افزار در جلوگیری از انتقال نرم‌افزاری که براساس قرارداد حق امتیاز شرینک رپ و کلیک رپ به فروش رسیده است.

۳) مقرره‌ای در این قانون هست که به مالیکن نرم‌افزار اجازه می‌دهد قراردادهای حق امتیاز شرینک رپ و کلیک رپ را بمحض گشودن بسته‌بندی یا کلیک بر کلمه «موافقم» بدون توجه به اینکه شروط هنوز خوانده نشده‌اند، نافذ شمرده و اجرا کنند[۶۶].

٤ـ مبنای غیر ارادی برای حمایت از مالک نرم‌افزار:

در دهه‌های قبل مالکین نرم‌افزار با توجه به تردید در اعتبار قرارداد شریک رپ به مبنای غیر قراردادی هم استناد می‌کردند و آن نقض حق مؤلف مالک نرم‌افزار است. بدین معنی که مطابق قاعده حقوق مالکیت فکری تنها کسی که حق تکثیر اثر فکری را دارد مؤلف آن می‌باشد و دیگران تنها درصورتی مجاز هستند که از جانب وی اجازه داشته باشند[۶۷]. استفاده از یک نرم‌افزار قهراً مستلزم تکثیر آن است: برای انکه نرم‌افزار نصب شود بایستی از دیسکت به حافظه کامپیوتر (هارد دیسک) کپی شود و هر بار که نرم‌افزار استفاده می‌شود عمل بکار انداختن (ruining) و لود کردن برنامه عمل تکثیر به شمار می‌رود: نتیجه آنکه خریدار

نرم‌افزار برای اینکه بتواند از آن بهره‌برداری کند و نقض حق مؤلف پیش نیاید ناچار است از مؤلف اجازه بگیرد و از آنجا که حدود اجازه و اذن وی در قرارداد بیان شده، قرارداد حق امتیاز نمایانگر همین اذن است ولو قانوناً نافذ نباشد.

این استدلال در حال حاضر طرفداران چندانی ندارد: مهم‌ترین اشکالی که بر این استدلال وارد شده مخالفت با نص قانون است: اصولاً قوانین حق مؤلف این اجازه را می‌دهند که کاربر مجاز بتواند در صورت ضرورت کپی تهیه کند[۶۸]. لذا این عمل نقض حقوق مؤلف محسوب نمی‌شود در حقوق انگلستان قانون حق مؤلف، حق طراحی و حق اختراع مصوب ۱۹۸۸ [۶۹] و قانون اصلاحی نظامات حق مؤلف (برنامه‌های کامپیوتری) مصوب ۱۹۹۲ [۷۰] بر این مطلب تأکید دارند. لذا استدلال مذکور مردود است[۷۱].

۵ـ اعتبار قراردادهای کلیک رپ و بروز رپ

در خاتمه بطور مختصر به مسأله اعتبار قراردادهای کلیک رپ و بروز رپ اشاره می‌کنیم. همانطور که قبلاً گفتیم در بین این سه قرارداد حق امتیاز از نظر اعتبار کلیک رپ در مقام اول و بروز رپ در مقام آخر است. از آنجایی که در کلیک رپ مشتری تا تمام شروط را نبیند و روی دگمه «موافقم» کلیک نکند این قرارداد یک قرارداد الزام‌آور است چرا که مشتری امکان مطالعه و بررسی کلیه شروط قرارداد را دارد و در صورت عدم تمایل می‌تواند بر روی کلمه «موافق نیستم» کلیک کرده و انصراف خود را از خرید نرم‌افزار اعلا کند. لذا دادگاه‌ها بارها بر اعتبار قرارداد کلیک رپ تأکید کرده‌اند: مثلاً دادگاه بدوی پرونده ProCD صراحتاً قرارداد کلیک رپ را قراردادی نافذ و معتبر شمرد[۷۲].

در مقابل قرارداد بروز رپ وضعیتی بدتر از قرارداد شرینک رپ دارد. بطوری که بجرأت می‌توان گفت رویه قضائی عدم اعتبار این قرارداد را پذیرفته است. در این قرارداد کاربر یا مشتری هیچ الزامی و اجباری به مطالعه شروط قرارداد ندارد و مجبور نیست برای اینکه بتواند نرم‌افزار را دان‌لود کند روی کلمه «موافقم» کلیک کند، بلکه بسادگی با کلیک بر کلمه دان لود می‌تواند نرم‌افزار را تحصیل کند، لذا هیچ توافق و تراضی شکل نگرفته و اراده یک طرفه مالک نرم‌افزار نمی‌تواند اجباری بر مشتری تحمیل کند. رویه قضایی در پرونده Specht, et al V. Netscape Communication et al سال ۲۰۰۱ بر عدم الزام‌آور بودن این قرارداد تأکید کرد. دادگاه شرط داوری موجود در این قرارداد را بلحاظ عدم الزام‌آور بودن خود قرارداد باطل شمرد[۷۳].

پی‌نوشت

۱. قانونگذار ایران در سال ۱۳۴۸ با تصویب قانون حمایت از مؤلفان، مصنفان و هنرمندان مفهوم حق مؤلف را در مورد کلیه آثار فکری من جمله نرم‌افزار کامپیوتری پذیرفت و در سال ۱۳۷۹ با تصویب قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای بطور اخص وجود حق مؤلف را برای نویسنده نرم‌افزار مورد شناسایی قرار داد.

۲. زرکلام، ستار: قراردادهای انفورماتیک چگونه مذاکره و منعقد کنیم دبیرخانه شورای عالی انفورماتیک آبان ۱۳۸۰ ش ۶۲

۳. برخی این رویه قبولی را « رویه قبولی بمحض گشودن» ترجمه کرده‌اند: زرکلام، ستار، همان، ش ۶۲

4. Reed, Chris; Computer Law, 2nd ed. (London; C.Reed, 1993) P.57
5. http:// WWW.lex 2k.org/Shrink Wrap/overveiw. PdF
6. http://WWW.nuslaw club.com/contract
7. Morgan, Richard; Borden, kit; computer contracts. Sweet & max well (London 2001) P.85
8. http://WWW.lex 2k.org (Ibid)
9. http://WWW.lex 2k.org (Ibid)
10. note 6. Supra
11. http: WWW 4.airnet.ne.jp/sage/data/doc/shrink.htm
12. note 7 supra P.98
13. Copyright Act 1976
14. computer software Rental Amendment Act 1990
15. http://WWW.fenwich.com/docstore/publications/Ip/Ip Aricles/Shrink Wrap.pdf

۱۶. (entire agreement) شرطی که بموجب آن طرفین توافق می‌کنند قرارداد کتبی تنها سند تراضی طرفین تلقی شود و بر تمام مکاتبات و مذاکرات قبلی حاکم باشد.

17. not 7. Supra P.9818.
18. Consumer Protection Act 1987
19. note 4 supra P. 58
20. Sales of Goods Act 1979
21. Uniform commercial code
22. note 7. Supra P.98
23. One-copy-on-one-CPU-at-a-time
24. note 11.supra
25. note 11.supra

۲۶. آیتی حمید، حقوق آفرینش‌های فکری نشر حقوقدان پاییز ۷۵، ص ۷۲

27. note 11. Supra
28. note 5. Supra
29. note 11. Supra
30. note 11. Supra
31. note 11. Supra
32. note 11. Supra
33. note 11. Supra
34. note 11. Supra

۳۵. میرمحمد صادقی، حسین: مروری بر حقوق قراردادها در انگلستان، نشر حقوقدان، سال ۱۳۷۷، ص ۳۱

۳۶. شهیدی، مهدی: تشکیل قراردادها و تعهدات، نشر مجد، سال ۱۳۸۰، ص ۱۵۵

۳۷. شماره ۳۶. بالا

۳۸. برای مطالعه بیشتر ر.ک به شماره ۳۵ صفحه ۴۸ به بعد

۳۹. گفته شده مفهوم عوض در حقوق کامن‌لا معادل مفهوم علت (La cause de l'obligation) در حقوق رومی ژرمنی است: رک به بهرامی احمدی، حمید: سوء استفاده از حق، ص ۲۲۴

40. Un fair contract terms Act 1977
41. consumer protection Act 1987
42. unreasonable
43. note 11. Supra

۴۴. این احتمالات عبارتند از ۱) قرارداد حق امتیاز با تولید کننده نرم‌افزار؛ ۲) قرارداد فروش کالا با توزیع کننده؛ ۳) قرارداد مرکب از حق امتیاز و فروش کالا با تولید کننده (توزیع کننده بعنوان عامل تولید کننده در نظر گرفته شده است؛ ۴) یک قرارداد منحصر بفرد جدید

Brain bridge, David, introduction to computer law

برای اطلاعات بیشتر ر.ک به Forth edition, (Longman; England) P. 234

۴۵. اصل نسبی بودن قراردادها به این معنی است که قراردادها رابطه حقوقی است بین دو طرف آن و کلیه حقوق و تکالیف و آثار ناشی از آن تنها دامنگیر طرفین قرارداد می‌شود.

برای مطالعه بیشتر ر.ک به شماره ۳۵ ص ۱۷۰ به بعد

و نیز کاتوزیان، ناصر: قواعد عمومی قراردادها، ج ۳، انتشارات بهشهر، خرداد ۶۸ ، ص ۲۷۵ به بعد

46. note 7. Supra P.99 & note 6 supra & note 11 supra
47. note 6. Supra
48. contract (Right of third party) 1999
49. note 7. Supra p.99
50. will theory
51. bargain theory
52. note 11. supra

۵۳. جهت تعدیل ظریه مذاکره گفته شده همین که طرفین امکان اطلاع یافتن از شروط قرارداد را داشته باشند کافی است ر.ک note 11. Supra

54. note 5. Supra
55. note 11. Supra
56. note 11. Supra

مضمون همین استدلال در ماده ۲B_۳۰۸ پیش‌نویس قانون اصلاح کد یکنواخت تجاری (UCC) ایالات متحده پذیرفته شده است.

57. note 11. Supra

58. pay now terms later
59. note 5. Supra
60. note 6. Supra & note 5. Supra & note 15. Supra
61. note 15. Supra
62. note 15. Supra
63. opportunity to inspect
64. note 15. Supra
65. uniform computer Information Transanction Act
66. http://WWW.shawpittman. com/news. Nsf/D/8525689000756690
    85256825005177e8/$file/tech//99.pdf

۶۷. در ماده یک قانون حمایت از پدیدآورندگان نرم‌افزارهای رایانه‌ای هم، تکثیر نرم‌افزار حق انحصاری پدید آورنده شناخته شده است.

۶۸. ماده ۷ قانون حمایت از پدیدآورندگان نرم‌افزارهای رایانه‌ای

69. Copyright, Designs and Patent Act 1998
70. Copyright Computer programs) Amendment Act 1995
71. note 7. Supra. P. 100
72. note 15. Supra
73. note 15. Supra & note 5. Supra &
http://shaw pittman. Com/news.nsf/(on-line Browse-Wrap licenses not binding)