جرائم رایانه ای؛ لزوم به روز بودن ساز و کارهای قانونی ..

با توجه به پیشرفت تکنولوژی و اطلاعات ، به طور یقین افرادی سودجو و فرصت طلب با فراگیری دانش درصدد سوء استفاده از تکنولوژی می باشند. این افراد، امکاناتی را که توسعه تکنولوژی برای جامعه بشری به ارمغان می آورد دست خوش امیال و اغراض خود ساخته و باعث ایجاد مشکلاتی برای استفاده کنندگان از تکنولوژی می گردند. ایجاد شبهه و تردید برای استفاده صحیح و به صرفه از این امکانات و تکنولوژی موضوعی است که امروزه توجه دولتمردان ، حقوق دانان ، متخصصین در امر تکنولوژی را به خود معطوف کرده است. بدیهی است تکنولوژی کامپیوتری هر چه بیشتر توسعه یابد جرائم کامپیوتری نیز توسعه پیدا خواهند نمود اما در وضعیت فعلی، قوانینی که بتواند با این جرائم برخورد نماید پاسخ‌گو نخواهد بود و دولتها می بایست قوانین خود را متناسب با جرایم تدوین نمایند.

توجه به اختلاف اساسی جرایم کامپیوتری با جرایم غیر کامپیوتری و کلاسیک در تصویب و اجرای قوانین امریست ضروری زیرا :

اولاً : شیوه ارتکاب آنها تقریباً آسان است .

ثانیاً : با منابعی اندک می توانند خسارات هنگفتی وارد نمایند .

ثالثاً : جرایم کامپیوتری معمولاً در عرصه بین المللی بوده و به سادگی مشخص نیست که کدام حوزه قضایی صلاحیت رسیدگی به جرم را بر عهده دارد .

رابعاً : با توجه به بین المللی بودن جرایم کامپیوتری ممکن است در بعضی از کشورها این موضوعات به عنوان جرم تلقی نگردیده و یا حتی قانونی مبنی بر مجازات متخلفان وجود نداشته باشد .

بررسی قوانین کیفری ایران پیرامون جرایم رایانه ای

بحث جرایم رایانه ای در ایران ابتدا در اوایل دهه ۱۳۸۰ مطرح شد. آن زمان بیشتر حوزه هایی را در بر می‌گرفت که به جعل اسناد دولتی و شخصی مربوط می شد. چنانکه اولین جرم رایانه‌ای در خرداد ۱۳۷۸ به ثبت رسید که در آن یک دانشجوی کامپیوتر و یک کارگر چاپخانه در کرمان، چک های تضمینی را جعل می‌کردند.

جعل اسکناس، بلیت شرکت های اتوبوسرانی، جعل اسناد دولتی از قبل گواهینامه رانندگی، کارت پایان خدمت، مدرک تحصیلی، اوراق خرید و فروش خودرو و چک های مسافرتی از دیگر موارد جرم رایانه ای در اوایل دهه ۸۰ به حساب می‌آمد.

با گسترش وسایل ارتباطی، کمیته‌ای با حضور وزارتخانه‌های اطلاعات، ارشاد، آموزش و پرورش، صداو سیما، ارتباطات و سازمان تبلیغات اسلامی تشکیل شد تا در باره فیلترینگ سایت‌ها تصمیم‌گیری کنند. در این زمان بحث اولیه در باره جرایم رایانه‌ای تا حد زیادی تغییر کرد.

متأسفانه در ایران موضوع تخلفات و جرایم کامپیوتری دیرتر از کشورهای دیگر نمودار گردیده و شاید علت آن ناشناخته بودن فن آوری اطلاغات در ایران بوده است. با توسعه فن آوری اطلاعات و فراگیر شدن آن در بین عموم مردم ، توجه مدیران کشور به وجود قوانین لازم معطوف گردید . اولین مرجع رسمی کشور که لزوم توجه به حقوق رایانه ای را احساس نمود شورای عالی انفورماتیک وابسته به سازمان برنامه و بودجه کشور بوده است . اولین قانونی که پیرامون جرائم کامپیوتری در ایران تصویب شد به سال ۱۳۷۹ بر می گردد که مجلس شورای اسلامی «قانون حمایت از پدید آورندگان نرم افزارهای رایانه ای » را تصویب نمود. در سال ۱۳۸۱ نیز طرح قانون تجارت الکترونیکی تهیه که نهایتاً متن آن در سال ۱۳۸۲ به تصویب نهایی مجلس شورای اسلامی رسید که رویکرد عمده ی آن، حمایت کیفری از حقوق مصرف کننده ، حمایت از داده ها و کپی رایت و ... بود.

در نهایت **قانون جرایم رایانه ای** در سال ۱۳۸۸ برای تعیین مصادیق استفاده مجرمانه از سامانه های رایانه‌ای و مخابراتی به تصویب مجلس شورای اسلامی رسید.کلیات لایحه قانون جرائم رایانه ای در ۲۷ آبان ۱۳۸۷ با ۱۷۶ رأی موافق، ۳ رأی مخالف و ۲ رأی ممتنع به تصویب رسید. پس از رفع ایراداتی که شورای نگهبان به این قانون وارد کرده بود در ۷ تیر ۱۳۸۸ قانون جرائم رایانه ای به تأیید شورای نگهبان رسید و رئیس‌جمهور ۱۰ تیر همان سال آن را برای اجرا ابلاغ کرد.

قانون جرایم رایانه‌ای در ۵ بخش و ۵۵ ماده تنظیم شده‌است. حبس و جریمه نقدی یا هر دو مجازات هایی است که برای مرتکبین این جرایم وضع شده است. جرایمی که در این قانون تعیین شده است شامل این موارد می‌گردد:

- دسترسی غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی
- شنود غیرمجاز
- جاسوسی رایانه‌ای

- جعل داده‌های قابل استناد یا ایجاد یا وارد کردن متقلبانه داده‌ها و تغییر داده‌ها یا علایم موجود در کارت‌های حافظه یا قابل پردازش در سیستم های رایانه‌ای یا مخابراتی یا تراشه ها یا ایجاد یا وارد کردن متقلبانهٔ داده‌ها یا علایم به آن‌ها
- تخریب و اخلال در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی دیگری
- سرقت و کلاهبرداری مرتبط با رایانه
- تولید، ارسال، انتشار، توزیع یا معامله داده‌های تصویر، صوت یا متن واقعی یا غیر واقعی با محتویات مستهجن
- تحریک، ترغیب، تهدید، دعوت، فریب یا آموزش ارتکاب جرائم منافی عفت یا استعمال مواد مخدر یا روان‌گردان یا خودکشی یا انحرافات جنسی یا اعمال خشونت‌آمیز
- هتک حیثیت و نشر اکاذیب، شامل تغییر یا تحریف و انتشار فیلم یا صوت یا تصویر دیگری - انتشار صوت یا تصویر یا فیلم خصوصی و خانوادگی دیگری بدون رضایت او و انتشار مطالب دروغ به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی
- تولید یا انتشار یا توزیع یا معامله داده ها یا نرم‌افزارها یا هر نوع ابزار الکترونیکی که صرفاً به منظور ارتکاب جرائم رایانه‌ای به کار می‌روند
- فروش یا انتشار یا در دسترس قرار دا دن گذرواژه یا هر داده ای که امکان دسترسی غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی متعلق به دیگری را فراهم می‌کند
- آموزش نحوهٔ ارتکاب جرایم دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای و تخریب و اخلال در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی

بر اساس ماده ۲۲ این قانون *کمیته تعیین مصادیق محتوای مجرمانه* شامل وزیر یا نمایندهٔ وزارتخانه‌های آموزش و پرورش، ارتباطات و فناوری اطلاعات، اطلاعات، دادگستری، علوم، تحقیقات و فناوری، فرهنگ و ارشاد اسلامی، رئیس سازمان تبلیغات اسلامی، رئیس سازمان صدا و سیما و فرمانده نیروی انتظامی، یک نفر خبره در فناوری اطلاعات و ارتباطات به انتخاب کمیسیون صنایع و معادن مجلس شورای اسلامی و یک نفر نمایندهٔ مجلس شورای اسلامی به انتخاب کمیسیون حقوقی و قضایی و تأیید مجلس شورای اسلامی می‌شود و ریاست کمیته به عهدهٔ دادستان کل کشور خواهد بود.

این کمیته در دی‌ماه ۱۳۸۸ فهرستی از مصداق‌های محتوای مجرمانه را ارائه داد. این فهرست در پنج فصل در بخش‌های " محتوی خلاف عفت و اخلاق عمومی، محتوی علیه مقدسات، محتوی علیه امنیت و آرامش عمومی، محتوی علیه مقامات و نهادهای دولتی و عمومی و محتوایی که برای ارتکاب جرایم رایانه‌ای و سایر جرایم" تهیه شده بود . بخشی از این فهرست به مواردی اشاره دارد که در قانون مجازات اسلامی نیز آمده‌است ولی در برخی موارد مصادیق ارائه‌شده تازگی دارد.

از جمله موارد ممنوع شده در این قانون انتشار فیلترشکن یا آموزش عبور از فیلترینگ می‌شود. این درحالی‌است که بسیاری از سایت‌ها در ایران فیلتر شده و کاربران با استفاده از فیلترشکن از این سایت ها استفاده می‌کنند. مورد دیگر آن که اگر کسی لینک سایت هایی را که دارای محتوی مجرمانه هستند یا در آن‌ها نشانی‌های اینترنتی سایت‌های مسدود شده و نشریات توقیف شده آمده را منتشر کند، مجرم است. به اشتراک گذاشتن لینک ها نیز از جمله کارهای مرسوم در اینترنت است که کاربران اینترنتی این گونه لینک‌ها را در سایت‌ها و وبلاگ‌ها قرار می‌دهند که بایست به آن توجه شود.

هشدار؛ آمارها سخن می گویند ..

به گفته ی رییس پلیس فتا در سال ۸۹ تعداد هزار و ۳۵ فقره جرم اینترنتی در ایران به ثبت رسیده که این آمار در سال ۹۰ به چهار هزار مورد افزایش یافته است و میزان این جرایم در سال ۹۱ به ۱۰هزار فقره رسیده است.

در خصوص بیشترین جرایم اینترنتی در کشور نزدیک به ۵۰ درصد از جرائم، برداشت از حساب بانکی است که این به جهت بی‌موالاتی مالکین در نگهداری رمزهایشان، سوء استفاده اینترنتی از حساب هایشان یا نفوذ هکر به شبکه بانکی و برداشت پول بوده است .

هتک حیثیت دومین جرم اینترنتی در کشور است که سردار هادیانفر نمونه آن را ارائه اطلاعات غلط از اساتید دانشگاه، دزدیدن عکس ها باستفاده از ایمیل های ایجاد شده و انتشار آن در سایت ها دانست .

رئیس پلیس فتا کلاهبرداری اینترنتی با استفاده از فیشینگ و فارمینگ را سومین جرم سایبری در کشور بیان می کند. (در فیشینگ سایتی کاملا شبیه درگاه اینترنتی یک بانک طراحی می‌شود؛ پس از ثبت رمز و پسورد حساب، اطلاعات حساب و رمزها به هکر منتقل می شود و وی بلافاصله با این اطلاعات حساب فرد را خالی می کند.)

به گزارش خبرگزاری ایسنا، متوسط دسترسی مردم به اینترنت در تمام استان ها بیش از ۳۰ درصد است و

در کشور، ۲۲ استان ضریب نفوذی بین ۳۰ تا ۶۰ درصد و ۹ استان هم بین ۶۰ تا ۹۰ درصد ضریب نفوذ دارند. با عنایت به جمیع جهات و با توجه به تعداد کاربران اینترنتی در کشور (قریب به ۴۰ میلیون نفر) و روند صعودی نرخ رشد جرائم و تهدیدات در فضای مجازی به نظر می رسد دقت و تامل قانونگذار و مسئولین اجرایی با دیدگاه پیشگیری و اصلاح روندها امری بایسته و ضروری است . ضمن آنکه ورود مراکز آموزشی و دانشگاهی و حوزه وسیع رسانه های دیداری و نوشتاری با هدف اطلاع رسانی و ارتقاء سطح آگاهی های عموم مردم، امریست تاثیرگذار که بایست برای آن وقت و بودجه کافی اختصاص یابد

در نهایت، پاسخ پژوهشگران و متخصصین امر به سوالات زیر می تواند راهگشای بسیاری از معضلات گذشته، حال و آینده در این حوزه باشد.

۱- آیا ساختار جامعه باعث بروز جرایم رایانه ای می شود ؟ و آیا اساسا نقش جامعه در شکل گیری چنین جرایمی مؤثر ا ست ؟

۲-آیا قانون جلوگیری از چنین جرمهایی بازدارندگی کافی را ندارند ؟

۳-آیا آزادی کارکنان در ادارات و شرکتها باعث این جرم ها می شود ؟

۴- آیا عدم آموزش لازم به مردم و کارکنان باعث بروز چنین جرمهایی می شود ؟

۵-آیا نداشتن امنیت کافی سیستمهای ادارات و شرکتها و افراد شخصی باعث دسترسی آسان افراد به آنها می شود؟

محمود کاتبی پور

کارشناس ارشد مدیریت فناوری اطلاعات و ارتباطات

سرپرست اداره برنامه ریزی و دبیرخانه شورای پیشگیری از وقوع جرم دادگستری استان آذربایجانشرقی