



حقوق جزای اختصاصی رایانه ای

مؤلفین

حجت محمد حسینی حاجیور

مدرس دانشگاه آزاد اسلامی اصفهان واحد خمینی شهر

دکتر امین امیریان فارسانی

دکترای حقوق کیفری و جرم شناسی و مدرس دانشگاه

انتشارات قانون یار

۱۳۹۸

| | |
|---------------------|--|
| سرشناسه | : امیریان فارسانی، امین، ۱۳۶۹ - |
| عنوان قراردادی | : ایران. قوانین و احکام Iran. Laws, etc |
| عنوان و نام پدیدآور | : حقوق جزای اختصاصی رایانه‌ای/مؤلفین امین امیریان فارسانی، حجت محمدحسینی حاجیور. |
| مشخصات نشر | : تهران: انتشارات قانون یار، ۱۳۹۸. |
| مشخصات ظاهری | : ۴۰۰ ص. |
| شابک | : ۹۷۸-۶۲۲-۲۲۹-۰۷۹-۵ |
| وضعیت فهرست نویسی | : فیپا |
| یادداشت | : کتابنامه: ص. ۳۹۱. |
| موضوع | : جرایم کامپیوتری -- قوانین و مقررات -- ایران |
| موضوع | : Computer crimes -- Law and legislation-- Iran |
| موضوع | : جعل -- قوانین و مقررات -- ایران |
| موضوع | : Forgery -- Law and legislation -- Iran |
| موضوع | : حقوق جزا -- ایران |
| موضوع | : Criminal law -- Iran |
| شناسه افزوده | : محمدحسینی حاجیور، حجت، ۱۳۶۸ - |
| رده بندی کنگره | : ۸۰-KMH |
| رده بندی دیویی | : ۵۵۰۹۹۴۴/۳۴۳ |
| شماره کتابشناسی ملی | : ۵۸۴۵۹۳۶ |

انتشارات قانون یار

حقوق جزای اختصاصی رایانه ای

تألیف: دکتر امین امیریان فارسانی - حجت محمد حسینی حاجیور

ناشر: قانون یار

ناظر فنی: محسن فاضلی

نوبت چاپ: اول - ۱۳۹۸

شمارگان: ۱۱۰۰ جلد

قیمت: ۷۰۰۰۰ تومان

شابک: ۹۷۸-۶۲۲-۲۲۹-۰۷۹-۵

مرکز پخش: تهران، میدان انقلاب، خ منیری جاوید، پلاک ۹۲

تلفن: ۶۶۹۷۹۵۱۹ مرکز پخش قانون یار

ماحصل آموخته‌هایم را تقدیم می‌کنم
به آنان که مهر آسمانی شان آرام بخش آلام زمینی ام است

به استوارترین تکیه‌گاهم، دستان پر مهر پدرم

به سبزترین نگاه زندگیم، چشمان گرم مادرم

به یادکاران تمام عمر، اساتیدم

که هرچه آموختم در کتب عشق شما آموختم و هرچه بگوختم قطره‌ای از دریای نبی کران مهربانان را پاس نتوانم بگویم
امروز هستی ام به امید شماست و فردا کلید باغ بهشتم رضای شما بهای کران سنگ تر از این ارزان نداشتم تا به خاک
پایان نثار کنم، باشد که حاصل تلاشم نسیم کوزه‌خوار حشمتیان را بزوداید. بوسه بردستان پر مهرتان

فهرست مطالب

| | |
|--|-----|
| بخش اول..... | ۱۷ |
| جایگاه جعل رایانه ای در حقوق کیفری ایران | ۱۷ |
| فصل اول: مفهوم شناسی ، پیشینه و مبانی جرم انگاری جعل رایانه ای | ۱۷ |
| ۱-۱- تعاریف و مفاهیم | ۱۷ |
| ۲-۱- جعل و تزویر سنتی (کلاسیک) | ۱۸ |
| ۳-۱- بزه کامپیوتری (بزه رایانه ای) | ۱۹ |
| گفتار سوم: رایانه - اینترنت - فضای سایبر | ۲۱ |
| ۴-۱- جعل رایانه‌ای | ۲۴ |
| ۱-۲- سیر تحول تاریخی جعل رایانه‌ای | ۲۷ |
| ۱-۱-۲- پیشینه تاریخی جعل رایانه‌ای در نظام حقوق بین‌الملل | ۲۸ |
| ۶-۱- پیشینه تاریخی جعل رایانه‌ای در حقوق جزای ایران | ۳۴ |
| فصل دوم: بررسی و تحلیل مبانی و عناصر تشکیل دهنده جعل رایانه ای | ۳۶ |
| ۱-۲- سیر تحول تاریخی جعل رایانه‌ای | ۳۶ |
| ۲-۲- مبانی بزه‌انگاری جعل رایانه‌ای | ۳۸ |
| ۳-۲- عناصر متشکله بزه جعل رایانه‌ای | ۴۰ |
| ۱-۳-۲- رکن قانونی | ۴۱ |
| ۲-۳-۲- رکن مادی | ۴۴ |
| موضوع بزه | ۵۸ |
| ۳-۳-۲- رکن معنوی (مفادی) | ۷۴ |
| فصل سوم: ضمانت‌اجراه‌های بزه جعل رایانه‌ای | ۷۷ |
| ۱-۳- بررسی توصیفی مسئولیت کیفری در فضای سایبر و جعل رایانه‌ای | ۷۸ |
| گفتار دوم: مسئولیت کیفری اشخاص حقوقی در جعل رایانه‌ای | ۸۲ |
| ۲-۳- مجازات در جعل رایانه ای | ۸۴ |
| فصل چهارم : قواعد شکلی ناظر بر جعل رایانه ای | ۹۰ |
| ۱-۴- تعقیب و رسیدگی جعل رایانه‌ای | ۹۰ |
| ۲-۴- بررسی صلاحیت کیفری در جعل رایانه‌ای | ۹۷ |
| بخش دوم..... | ۱۱۵ |
| جایگاه حقوقی خرابکاری رایانه ای | ۱۱۵ |
| فصل اول: مفهوم شناسی ، پیشینه و قرین شناسی خرابکاری رایانه ای | ۱۱۸ |



- ۱۱۸-۱- مفهوم شناسی ۱۱۸
- ۱۱۸-۱-۱- خرابکاری ۱۱۸
- ۱۲۱-۱- فضای سایبر ۱۲۱
- ۱۲۵-۲- پیشینه شناسی ۱۲۵
- ۱۲۷-۳- خرابکاری رایانه ای در قوانین سایرکشورها ۱۲۷
- ۱۳۰-۴- خرابکاری رایانه ای در اسناد بین المللی ۱۳۰
- ۱۳۲-۵- قرین شناسی ۱۳۲
- ۱۳۲-۱-۵- اخلال سامانه ای ۱۳۲
- ۱۳۳-۲-۵- اتلاف داده ۱۳۳
- ۱۳۵-۳-۵- تروریسم سایبری ۱۳۵
- ۱۳۸-۴-۵- وندالیسم ۱۳۸
- ۱۴۰- فصل دوم: عناصر متشکله بزه خرابکاری رایانه ای ۱۴۰
- ۱۴۵-۲- رکن مادی ۱۴۵
- ۱۴۵-۱-۲- رفتار مجرمانه ۱۴۵
- ۱۴۶-۲-۲- تخریب ۱۴۶
- ۱۴۸-۳-۲- اخلال ۱۴۸
- ۱۵۲-۴-۲- ممانعت ۱۵۲
- ۱۵۳-۳- موضوع جرم ۱۵۳
- ۱۵۳-۱-۳- داده ۱۵۳
- ۱۵۸-۴- نتیجه مجرمانه ۱۵۸
- ۱۶۱-۵- شرایط و اوضاع و احوال جرم ۱۶۱
- ۱۶۱-۱-۵- بستر ارتکاب جرم: فضای سایبر ۱۶۱
- ۱۶۶-۲-۵- تعلق داده یا سامانه به دیگری ۱۶۶
- ۱۶۷-۳-۵- ویژگی غیر مجاز بودن ۱۶۷
- ۱۶۹-۶- رکن روانی ۱۶۹
- ۱۶۹-۱-۶- علم ۱۶۹
- ۱۶۹-۲-۶- عمد عام ۱۶۹
- ۱۷۰-۳-۶- عمد خاص ۱۷۰
- ۱۷۱-۴-۶- انگیزه ۱۷۱
- ۱۷۳- فصل چهارم: ضمانت اجراهای خرابکاری رایانه ای ۱۷۳
- ۱۷۳-۱-۴- ضمانت اجرای کیفری ۱۷۳
- ۱۷۴-۱-۱-۴- مجازات اصلی ۱۷۴



| | |
|-----|------------------------|
| ۱۷۷ | ۲-۱-۴ مجازات ترمیمی |
| ۱۷۸ | ۳-۱-۴ مجازات تبعی |
| ۱۸۰ | ۲-۴ ضمانت اجرای تأمینی |
| ۱۸۲ | ۳-۴ ضمانت اجرای ترمیمی |
| ۱۸۵ | نتیجه گیری |

بخش سوم..... ۱۹۱

| | |
|-----|---|
| ۱۹۱ | تحلیل ممانعت از دسترسی به داده و سامانه در حقوق کیفری |
| ۱۹۲ | فصل اول: جایگاه حقوقی دسترسی به داده و سامانه |
| ۱۹۳ | ۱-۱- مفهوم شناسی |
| ۱۹۷ | ۲-۱- مبانی حق دسترسی به داده و سامانه |
| ۱۹۷ | ۱-۲-۱- نظریه حقوق بشر |
| ۱۹۸ | ۲-۲-۱- نظریه پیمان با همادی (قرارداد اجتماعی) |
| ۲۰۰ | ۳-۲-۱- مبانی اخلاقی |
| ۲۰۲ | فصل دوم: عناصر متشکله بزه ممانعت از دسترسی به داده و سامانه |
| ۲۰۲ | ۱-۲- رکن قانونی |
| ۲۰۴ | ۲-۲- رکن مادی |
| ۲۰۶ | ۱-۲-۲- موضوع جرم |
| ۲۰۷ | ۲-۲-۲- شیوه های ارتکاب جرم ممانعت از دسترسی |
| ۲۰۷ | ۱-۲-۲-۱- ویروس های رایانه ای |
| ۲۰۷ | ۲-۲-۲-۲- تراواها |
| ۲۰۸ | ۳-۲-۲-۲- کرم های کامپیوتری |
| ۲۰۸ | ۴-۲-۲-۲- رمز نگاری |
| ۲۱۰ | ۳-۲- رکن روانی |
| ۲۱۰ | ۱-۳-۲- قصد عام |
| ۲۱۱ | ۲-۳-۲- علم |
| ۲۱۲ | ۳-۳-۲- قصد خاص |
| ۲۱۵ | ۴-۲- ویژگی های عمومی جرم ممانعت از دسترسی به داده و سامانه |
| ۲۱۵ | ۱-۴-۲- غیرمجاز بودن دسترسی به داده و سامانه |
| ۲۱۷ | ۲-۴-۲- رایانه ای بودن محض جرم ممانعت از دسترسی |
| ۲۱۹ | فصل سوم: ضمانت اجرای ممانعت از دسترسی به داده و سامانه |
| ۲۲۰ | ۱-۳- ضمانت اجرای کیفری اصلی |



- ۲۲۵ ۲-۳ - ضمانت اجرای کیفری غیر اصلی
- ۲۲۵ ۱-۲-۳ - مجازات تکمیلی
- ۲۲۷ ۲-۲-۳ - مجازات تبعی
- ۲۲۹ ۳-۳ - ضمانت اجرای تامینی
- ۲۳۱ ۴-۳ - ضمانت اجرای جبرانی (ترمیمی)
- ۲۳۳ ۱-۴-۳ - بیمه سایبری:
- ۲۳۵ نتیجه گیری
- ۲۳۹ پیشنهادات قانونی
- ۲۴۰ پیشنهادات اجرایی
- بخش چهارم..... ۲۴۳**
- ۲۴۳ جایگاه تروریسم سایبری در حقوق کیفری با رویکرد پیشگیری
- ۲۴۹ فصل اول : مفهوم شناسی ، تاریخچه ، عناصر تروریسم سایبری
- ۲۵۵ ۱-۱ - رفتار : اخلال و تخریب
- ۲۵۹ ۲-۱ - سامانه های ارایه دهنده خدمات ضروری
- ۲۶۰ ۳-۱ - رکن روانی
- فصل دوم: راهکارهای پیشگیری از بزه‌دیدگان تروریسم سایبری در حقوق کیفری ایران و اسناد بین‌المللی
- ۲۶۱ بین‌المللی
- ۲۶۱ ۱-۲ - راهکارهای پیشگیری از بزه‌دیدگان تروریسم سایبری در حقوق کیفری ایران
- ۲۶۲ ۱-۱-۲ - پیشگیری واکنشی یا کیفری
- ۲۶۳ ۱-۱-۱-۲ - قانون جرایم رایانه‌ای مصوب ۱۳۸۸
- ۲۶۷ ۲-۱-۱-۲ - قانون تجارت الکترونیکی مصوب ۱۳۸۲
- ۲۶۸ ۳-۱-۱-۲ - قانون مجازات نیروهای مسلح مصوب ۱۳۸۲
- ۲۶۹ ۴-۱-۱-۲ - قانون مجازات اسلامی مصوب ۱۳۷۰
- ۲۷۰ ۵-۱-۱-۲ - سایر قوانین و مقررات موجود
- ۲۷۰ ۱-۵-۱-۱-۲ - قانون راجع به مجازات اخلال‌گران در صنایع نفت مصوب ۱۶ مهر ۱۳۳۶
- ۲۷۰ ۲-۵-۱-۱-۲ - قانون مجازات اخلال‌گران در تأسیسات آب، برق، گاز و مخابرات کشور مصوب ۱۲ دی ماه ۱۳۵۱
- ۲۷۲ ۳-۵-۱-۱-۲ - قانون مجازات اخلال‌کنندگان در امنیت پرواز هواپیما و خرابکاری در وسایل و تأسیسات هواپیمایی مصوب ۱۳۴۹
- ۲۷۳ ۴-۵-۱-۱-۲ - قانون الحاق دولت ایران به کنوانسیون جلوگیری از اعمال غیرقانونی علیه امنیت هواپیمایی کشوری مصوب ۱۳۵۲
- ۲۷۳ ۱۳۵۲



| | |
|--|-----|
| ۱-۱-۱-۵-۵- قانون تصویب پروتکل جلوگیری از اعمال خشونت آمیز در فرودگاه‌های در خدمت هواپیمایی کشوری | ۲۷۴ |
| ۱-۱-۱-۶-۵- قانون کیفر بزه‌های مربوط به راه آهن مصوب ۳۱ فروردین ۱۳۲۰ و اصلاحات بعدی | ۲۷۵ |
| ۱-۱-۱-۷-۵- لایحه مبارزه با تروریسم | ۲۷۶ |
| ۲-۱-۲- پیشگیری غیر کیفری | ۲۷۶ |
| ۱-۲-۱-۲- پیشگیری اجتماعی | ۲۷۷ |
| ۱-۲-۱-۲-۱-۲- پیشگیری اجتماعی جامعه مدار | ۲۷۷ |
| ۱-۱-۱-۲-۱-۲- برنامه جامع توسعه تجارت الکترونیکی مصوب ۱۳۸۴ | ۲۷۸ |
| ۱-۲-۱-۲-۲- برنامه چهارم توسعه مرتبط به فناوری اطلاعات | ۲۷۹ |
| ۱-۲-۱-۲-۳-۱-۲-۱-۲- قانون برنامه پنج ساله پنجم توسعه جمهوری اسلامی ایران | ۲۷۹ |
| ۱-۲-۱-۲-۴-۱-۲-۱-۲- مقررات و ضوابط شبکه‌های اطلاع رسانی رایانه‌ای | ۲۸۰ |
| ۱-۲-۱-۲-۵-۱-۲-۱-۲- ابلاغیه مقام معظم رهبری درباره سیاست‌های کلی شبکه‌های اطلاع رسانی رایانه‌ای | ۲۸۱ |
| ۱-۲-۱-۲-۶-۱-۲-۱-۲- مصوبه شورای عالی اداری در خصوص اتوماسیون نظام اداری و اتصال به شبکه جهانی اطلاع رسانی | ۲۸۱ |
| ۱-۲-۱-۲-۷-۱-۲-۱-۲- سیاست تجارت الکترونیکی جمهوری اسلامی ایران | ۲۸۲ |
| ۱-۲-۱-۲-۸-۱-۲-۱-۲- سند راهبردی امنیت فضای تبادل اطلاعات مصوب ۱۳۸۴ | ۲۸۲ |
| ۱-۲-۱-۲-۲-۱-۲-۲- پیشگیری اجتماعی رشدمدار | ۲۸۲ |
| ۱-۲-۲-۲-۱-۲-۲- پیشگیری وضعی | ۲۸۴ |
| ۱-۲-۲-۱-۲-۲-۱-۲- اقدامات فنی | ۲۸۴ |
| ۱-۲-۲-۱-۲-۲-۱-۲- تدابیر فنی پیشگیرانه در سازمان‌ها و ادارات کشور | ۲۸۵ |
| ۱-۲-۲-۱-۲-۲-۱-۲-۲- نصب و استقرار دیوار آتشین | ۲۸۵ |
| ۱-۲-۲-۱-۲-۲-۱-۲-۲- سیستم‌های تشخیص نفوذ | ۲۸۷ |
| ۱-۲-۲-۱-۲-۲-۱-۲-۲- سیستم‌های پیشگیری از نفوذ | ۲۸۸ |
| ۱-۲-۲-۱-۲-۲-۱-۲-۲- استفاده از برنامه‌های ضد ویروس | ۲۸۹ |
| ۱-۲-۲-۱-۲-۲-۱-۲-۲- استفاده از پروتکل‌های رمزگذاری | ۲۹۱ |
| ۱-۲-۲-۱-۲-۲-۱-۲-۲- پروتکل HTTPS | ۲۹۱ |
| ۱-۲-۲-۱-۲-۲-۱-۲-۲- پروتکل و گواهینامه دیجیتال SSL | ۲۹۲ |
| ۱-۲-۲-۱-۲-۲-۱-۲-۲-۱-۲-۲- پالایش یا فیلترینگ | ۲۹۲ |
| ۱-۲-۲-۱-۲-۲-۱-۲-۲-۱-۲- راه‌اندازی مرکز داده | ۲۹۳ |
| ۱-۲-۲-۱-۲-۲-۱-۲-۲-۱-۲- طرح شبکه ملی اطلاعات | ۲۹۴ |



- ۲۹۴ ۱-۲-۲-۱-۱-۱۱- اینترانت
- ۲۹۴ ۱-۲-۲-۱-۱-۱۲- تولید نرم افزارهای بومی
- ۲۹۵ ۱-۲-۲-۱-۱-۱۲- سیستم عامل قاصدک
- ۲۹۵ ۱-۲-۲-۱-۱-۱۲- نرم افزار (PVT Pro)
- ۲۹۵ ۱-۲-۲-۱-۱-۱۲-۳- موتور جستجوی پارسی جو
- ۲۹۶ ۱-۲-۲-۱-۱-۱۲-۴- پست الکترونیکی بومی
- ۲۹۶ ۱-۲-۲-۱-۲- اقدامات سازمان‌ها و مؤسسات
- ۲۹۷ ۱-۲-۲-۱-۲- وزارت ارتباطات و فناوری اطلاعات
- ۲۹۷ ۱-۲-۲-۱-۲- سازمان تنظیم مقررات و ارتباطات رادیویی
- ۲۹۸ ۱-۲-۲-۱-۲-۳- شرکت ارتباطات زیرساخت
- ۲۹۸ ۱-۲-۲-۱-۲-۴- سازمان فناوری اطلاعات
- ۲۹۹ ۱-۲-۲-۱-۲-۵- کارگروه مبارزه با ویروس‌های صنعتی جاسوسی
- ۲۹۹ ۱-۲-۲-۱-۲-۶- قرارگاه دفاع سایبری
- ۲۹۹ ۱-۲-۲-۱-۲-۷- مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای (ماهر)
- ۳۰۰ ۱-۲-۲-۱-۲-۸- سازمان پدافند غیرعامل
- ۳۰۱ ۱-۲-۲-۱-۲-۹- پلیس فضای تولید و تبادل اطلاعات ناجا
- ۳۰۲ ۱-۲-۲-۱-۲-۱۰- سازمان بررسی جرایم سازمان یافته
- ۳۰۴ ۱-۲-۲-۱-۲-۱۱- انجمن رمز ایران
- ۳۰۵ ۱-۲-۲-۱-۲-۱۲- مرکز ملی فضای مجازی
- ۳۰۵ ۲-۲- راهکارهای پیشگیری از بزه‌دیدگان تروریسم سایبری در اسناد بین‌المللی
- ۳۰۶ ۱-۲-۲- اقدامات پیشگیرانه کیفی در اسناد بین‌المللی و منطقه‌ای
- ۳۰۸ ۱-۲-۲-۱- کنوانسیون راجع به جلوگیری از اعمال غیرقانونی علیه امنیت هواپیمایی کشوری
- ۳۱۰ ۲-۲-۱-۲- کنوانسیون جلوگیری از بمب‌گذاری تروریستی
- ۳۱۱ ۲-۲-۱-۳- کنوانسیون سرکوب حمایت مالی از تروریسم
- ۳۱۳ ۲-۲-۱-۴- کنوانسیون توكيو راجع به جرائم و برخی از اعمال ارتكابی دیگر در هواپیما
- ۳۱۳ ۲-۲-۱-۵- قطعنامه شماره ۱۳۷۳ شورای امنیت
- ۳۱۴ ۲-۲-۱-۶- اعلامیه راجع به اقدامات ناظر به محای تروریسم بین‌المللی
- ۳۱۴ ۲-۲-۱-۷- راهبرد جهانی ضد تروریسم سازمان ملل متحد در سال ۲۰۰۵
- ۳۱۵ ۲-۲-۱-۸- بیانیه یازدهمین نشست پیشگیری از جرایم و بسط عدالت کیفری سازمان ملل متحد در سال ۲۰۰۵
- ۳۱۸ ۲-۲-۱-۱۰- کنوانسیون منطقه‌ای سازمان همکاری‌های منطقه‌ای آسیای جنوبی
- ۳۱۹ ۲-۲-۱-۱۱- کنوانسیون سازمان کنفرانس اسلامی در زمینه مبارزه با تروریسم بین‌المللی



| | |
|--|-----|
| ۱۲-۱-۲-۲- معاهده همکاری میان دولت‌های عضو کشورهای مستقل مشترک‌المنافع در مبارزه با تروریسم | ۳۲۱ |
| ۱۳-۱-۲-۲- کنوانسیون سازمان وحدت آفریقا درباره پیشگیری و مبارزه با تروریسم و پروتکل سال ۲۰۰۴ الحاقی به آن | ۳۲۳ |
| ۱۶-۱-۲-۲- کنوانسیون سازمان کشورهای آمریکایی راجع به پیشگیری و مجازات اعمال تروریستی | ۳۳۰ |
| ۱۷-۱-۲-۲- قطعنامه ایجاد فرهنگ جهانی امنیت سایبری و تلاش‌های ملی برای حفاظت از زیرساخت‌های اطلاعاتی حساس | ۳۳۱ |
| ۱۸-۱-۲-۲- قطعنامه ایجاد فرهنگ جهانی در رابطه با امنیت سایبر | ۳۳۲ |
| ۱۹-۱-۲-۲- قطعنامه مبارزه با سوءاستفاده جنایتکارانه از فناوری اطلاعات | ۳۳۲ |
| ۲۰-۱-۲-۲- قطعنامه ایجاد فرهنگ جهانی امنیت سایبر و حمایت از زیرساخت‌های اطلاعاتی حساس | ۳۳۳ |
| ۲-۲-۲- اقدامات پیشگیرانه غیر کیفری در اسناد بین‌المللی و منطقه‌ای | ۳۳۴ |
| ۱-۲-۲-۲- توصیه نامه‌های نشریه بین‌المللی سیاست جنایی | ۳۳۵ |
| ۲-۲-۲-۲- دستورالعمل و توصیه نامه‌های سازمان همکاری و توسعه اقتصادی | ۳۳۶ |
| ۳-۲-۲-۲- هشتمین نشست سازمان ملل متحد درباره پیشگیری از جرم و اصلاح مجرمین | ۳۴۰ |
| ۴-۲-۲-۲- راهبرد جهانی ضد تروریسم سازمان ملل متحد در سال ۲۰۰۶ | ۳۴۱ |
| ۳-۲-۲- اقدامات سازمان‌های بین‌المللی و منطقه‌ای | ۳۴۱ |
| ۱-۳-۲-۲- اقدامات اتحادیه بین‌المللی مخابرات | ۳۴۱ |
| ۲-۳-۲-۲- گروه کاری اطلاعات و ارتباطات همکاری اقتصادی آسیا و اقیانوس آرام | ۳۴۲ |
| ۳-۳-۲-۲- سازمان پلیس جنایی بین‌الملل | ۳۴۳ |
| ۴-۳-۲-۲- گروه جی هشت | ۳۴۴ |
| ۶-۳-۲-۲- سازمان امنیت و همکاری اروپا | ۳۴۴ |
| ۷-۳-۲-۲- مؤسسه بین‌المللی همکاری در مقابل تهدیدات سایبری | ۳۴۵ |
| ۸-۳-۲-۲- سازمان ناتو | ۳۴۶ |
| فصل سوم: روش‌های حمایت از بزه‌دیدگان تروریسم سایبری در حقوق کیفری ایران و اسناد بین‌المللی | ۳۴۶ |
| ۱-۳-۱-۱-۱- روش‌های حمایت از بزه‌دیدگان تروریسم سایبری در حقوق کیفری ایران | ۳۴۶ |
| ۱-۱-۱-۱-۱- حمایت کیفری | ۳۴۷ |
| ۱-۱-۱-۱-۱-۱- حمایت کیفری ساده | ۳۴۸ |
| ۱-۱-۱-۱-۱-۱-۱- قانون جرایم رایانه‌ای مصوب ۱۳۸۸ | ۳۴۹ |
| ۲-۱-۱-۱-۱-۱- قانون تجارت الکترونیکی مصوب ۱۳۸۲ | ۳۵۴ |



- ۳۵۴ ۱-۱-۱-۳- قانون مجازات اسلامی مصوب ۱۳۷۰
 ۱-۱-۱-۳-۴- قانون مجازات اخلاص گران در تأسیسات آب، برق، گاز و مخابرات کشور مصوب ۱۲ دی
 ماه ۱۳۵۱ ۳۵۶
 ۱-۱-۱-۳-۵- قانون راجع به مجازات اخلاص گران در صنایع نفت مصوب ۱۶ مهر ۱۳۳۶ ۳۵۷
 ۱-۱-۱-۳-۶- قانون کیفر بزه‌های مربوط به راه آهن مصوب ۳۱ فروردین ۱۳۲۰ و اصلاحات بعدی
 ۳۵۹
 ۱-۱-۲-۳-۲- حمایت کیفری ویژه یا افتراقی ۳۶۰
 ۱-۱-۲-۱-۳-۱- قانون جرایم رایانه‌ای مصوب ۱۳۸۸ ۳۶۰
 ۱-۱-۲-۱-۳-۲- قانون تجارت الکترونیکی مصوب ۱۳۸۲ ۳۶۱
 ۱-۱-۲-۱-۳-۳- قانون مجازات اخلاص گران در تأسیسات آب، برق، گاز و مخابرات کشور مصوب ۱۲ دی
 ماه ۱۳۵۱ ۳۶۱
 ۱-۱-۲-۱-۳-۴- قانون راجع به مجازات اخلاص گران در صنایع نفت مصوب ۱۶ مهر ۱۳۳۶ ۳۶۲
 ۱-۱-۳-۳-۱- حمایت کیفری دنباله‌دار ۳۶۲
 ۱-۱-۳-۱-۳-۱- قانون جرایم رایانه‌ای مصوب ۱۳۸۸ ۳۶۳
 ۲-۳-۲- روش‌های حمایت از بزه‌دیدگان تروریسم سایبری در اسناد بین‌المللی ۳۶۳
 ۱-۲-۳-۱- حمایت کیفری ۳۶۴
 ۱-۱-۲-۳-۱- کنوانسیون جرایم سایبر شورای اروپا ۳۶۵
 ۲-۱-۲-۳-۲- کنوانسیون راجع به جلوگیری از اعمال غیرقانونی علیه امنیت هواپیمایی کشوری ۳۶۶
 ۳-۱-۲-۳-۳- کنوانسیون جلوگیری از بمب‌گذاری تروریستی ۳۶۷
 ۴-۱-۲-۳-۴- کنوانسیون سرکوب حمایت مالی از تروریسم ۳۶۸
 ۵-۱-۲-۳-۵- کنوانسیون توکیو راجع به جرائم و برخی از اعمال ارتكابی دیگر در هواپیما ۳۶۹
 ۶-۱-۲-۳-۶- قطعنامه شماره ۱۳۷۳ شورای امنیت ۳۶۹
 ۷-۱-۲-۳-۷- راهبرد جهانی ضد تروریسم سازمان ملل متحد در سال ۲۰۰۵ ۳۷۰
 ۸-۱-۲-۳-۸- بیانیه یازدهمین نشست پیشگیری از جرایم و بسط عدالت کیفری سازمان ملل متحد در
 سال ۲۰۰۵ ۳۷۰
 ۹-۱-۲-۳-۹- کنوانسیون اروپایی مقابله با تروریسم ۳۷۱
 ۱۰-۱-۲-۳-۱۰- کنوانسیون منطقه‌ای سازمان همکاری‌های منطقه‌ای آسیای جنوبی ۳۷۲
 ۱۱-۱-۲-۳-۱۱- کنوانسیون سازمان کنفرانس اسلامی در زمینه مبارزه با تروریسم بین‌المللی ۳۷۳
 ۱۲-۱-۲-۳-۱۲- معاهده همکاری میان دولت‌های عضو کشورهای مستقل مشترک‌المنافع در مبارزه با
 تروریسم ۳۷۳
 ۱۳-۱-۲-۳-۱۳- کنوانسیون سازمان وحدت آفریقا درباره پیشگیری و مبارزه با تروریسم و پروتکل سال
 ۲۰۰۴ الحاقی به آن ۳۷۴



| | |
|-----|---|
| ۳۷۵ | کنوانسیون عربی مقابله با تروریسم |
| ۳۷۶ | کنوانسیون سازمان کشورهای آمریکایی راجع به پیشگیری و مجازات اعمال تروریستی |
| ۳۷۷ | قطعنامهٔ ایجاد فرهنگ جهانی امنیت سایبری و تلاش‌های ملی برای حفاظت از زیرساخت‌های اطلاعاتی حساس |
| ۳۷۷ | قطعنامهٔ مبارزه با سوءاستفادهٔ جنایتکارانه از فناوری اطلاعات |
| ۳۷۷ | قطعنامهٔ ایجاد فرهنگ جهانی امنیت سایبر و حمایت از زیرساخت‌های اطلاعاتی حساس |
| ۳۷۸ | کنوانسیون بین‌المللی حقوق مدنی و سیاسی |
| ۳۷۸ | قطعنامهٔ راجع به حمایت از قربانیان تخلفات فاحش بین‌المللی از قواعد بشر بین‌المللی و تخلفات جدی از حقوق بشردوستانهٔ بین‌المللی |
| ۳۷۹ | نشست هفتم سازمان ملل متحد دربارهٔ پیشگیری از جرم و اصلاح مجرمان |
| ۳۷۹ | حمایت‌های مدنی |
| ۳۷۹ | حمایت مادی |
| ۳۸۰ | کنوانسیون پیشگیری از تروریسم شورای اروپا |
| ۳۸۰ | کنوانسیون منع حمایت مالی از تروریسم |
| ۳۸۱ | توصیه‌نامهٔ کمیتهٔ وزیران عضو اتحادیهٔ اروپا برای حمایت از قربانیان جرایم |
| ۳۸۱ | راهبرد جهانی ضد تروریسم سازمان ملل متحد در سال ۲۰۰۵ |
| ۳۸۱ | حمایت‌های پزشکی |
| ۳۸۴ | حمایت شکلی |
| ۳۸۴ | کنوانسیون جرایم سایبر |
| ۳۸۶ | نتیجه‌گیری و پیشنهادات |
| ۳۸۶ | جمع بندی و پیشنهادات |
| ۳۸۸ | پیشنهادات |
| ۳۹۲ | منابع و مآخذ |

بخش اول

جایگاه جعل رایانه ای در حقوق کیفری ایران

فصل اول: مفهوم شناسی، پیشینه و مبانی جرم انگاری جعل رایانه ای

اگرچه بزه جعل رایانه‌ای به صورت یک عنوان جزایی جدید پا به عرصه نظام کیفری ایران گذاشته است ولی همانند سایر عناوین جزایی واجد کلیاتی می‌باشد که در واقع ذکر این کلیات، زمینه پرداختن به عناصر متشکله این بزه و همچنین تجزیه و تحلیل آن را مهیا می‌سازد. در واقع بزه جعل رایانه‌ای به عنوان یکی از جرائم رایانه‌ای دارای پیشینه و مبانی می‌باشد که ذکر آن در این فصل ضروری به نظر می‌رسد.

۱-۱- تعاریف و مفاهیم

از جمله جرایمی که در آن رایانه هم وسیله ارتکاب بزه است و هم موضوع آن، جعل رایانه‌ای است. «جعل در لغت به معنای دگرگون کردن، منقلب نمودن، قراردادن، آفریدن و وضع کردن، ساختن و ایجاد کردن به کار رفته است»^۱ امروزه به دلیل گسترش ارتباطات تجاری، سیاسی و علمی از یک طرف اعتبار و ارزش اسناد بسیار بیشتر از گذشته گردیده است که به همین دلیل جعل این اسناد با پاسخ شدید جامعه مواجه می‌باشد و از طرف دیگر به دلیل هزینه‌های نگهداری اسناد نوشته، بسیاری از مبادلات در جهان به وسیله اسناد الکترونیکی صورت می‌گیرد به طوری که

^۱ - معین، محمد، فرهنگ فارسی، تهران، امیرکبیر، ۱۳۷۵



تمام داد و ستدهای تجاری در بعضی از بنادر جنوب شرقی آسیا فقط با اینگونه اسناد صورت می‌پذیرد. «اسناد الکترونیکی دارای خصوصیتی می‌باشند که آنها را از دلایل و مدارک کاغذی سنتی متمایز می‌سازد»^۱ مهمترین خصوصیت نسخه الکترونیکی یک سند این است که می‌تواند با تصویری که از آن برداشته شده یکسان نباشد، امکان دارد فقط در جریان بررسی نسخه الکترونیکی، اطلاعات مخفی شده مهم آن قابل رؤیت باشد، در نتیجه داشتن تصویر الکترونیکی یک سند یا مدرک می‌تواند نسبت به نسخه به ظاهر کامل آن، اطلاعات بیشتری را به ما ارائه دهد. همچنین داده‌های الکترونیکی را می‌توان به صورت بسیار فشرده‌ای ذخیره کرد و این عمل باعث می‌شود که نقل و انتقال داده‌های الکترونیکی و از بین رفتن آنها نسبت به دلایل و مدارک کاغذی آسان‌تر شود و داده‌های الکترونیکی نسبت به اسناد و مدارک کاغذی آسیب‌پذیرتر هستند و در مقایسه با اطلاعات مندرج در پرونده‌های کاغذی به آسانی می‌توان این داده‌ها را دستکاری یا جعل کرد، ضمن اینکه این دستکاری را می‌توان با استفاده از دانش فنی مناسب راحت‌تر پنهان داشت. در مورد دلایل و مدارک میزخانه کاغذی، معمولاً افراد به تنهایی می‌توانند مدارک در دسترس را بازبینی کنند و موارد و مطالب دال بر مزهیت را به راحتی تخریب کرده یا تغییر دهند، با ظهور رایانه انجام این امور نیز پیچیده‌تر شده است. «هنوز این امکان وجود دارد که بتوان دلایل و مدارک موجود در قالب‌های الکترونیکی را دستکاری یا پاک کرد، اما برای سرپوش گذاشتن بر این دستکاری یا تخریب اساسی ادله الکترونیکی نیاز به کمک یک متخصص رایانه است»^۲ در اینجا به تعریف و شناسایی برخی از واژه‌های کلیدی که در این نوشته نقش اساسی داشته و به نوعی با جعل رایانه‌ای ارتباط دارند می‌پردازیم.

۱-۲- جعل و تزویر سنتی (کلاسیک)

از لحاظ اصطلاحی جعل و تزویر گاهی در یک مفهوم عام به کار برده می‌شود و گاهی در مفهوم خاص. در مفهوم عام هر نوع وارونه جلوه دادن حقیقت و واقعیت را جعل و تزویر گویند و در مفهوم خاص هر نوع وارونه جلوه دادن حقیقت در اسناد را جعل و تزویر گویند و «به عنوان

^۱ - گاتن آگن، ادله الکترونیکی، ترجمه مصیب رضائی تهران، شورای عالی توسعه قضایی، شورای عالی اطلاع‌رسانی ۸۳

^۲ - حسن نامی، رایانه و جعل اسناد الکترونیکی، مراجعه به اینترنت



یک اصل، جعل و تزویر بزه اسنادی است^۱ غالب قوانین جزایی بدون اینکه تعریف جامعی از جعل ارایه دهند و ارکان بزه جعل را دقیقاً تعیین کنند صرفاً به ذکر و احصای شیوه‌ها و راههای مختلف ارتکاب جعل بسنده کرده‌اند. با وجود این هر یک از استادان حقوق جزا تعریفی در این مورد ارایه کرده‌اند:

دکتر ابراهیم پاد بزه جعل را چنین تعریف کرده است: «جعل و تزویر عبارت است از قلب متقابلانه حقیقت به ضرر دیگری در یک سند یا نوشته یا چیز دیگر به یکی از طرق مذکور در قانون»^۲ یکی دیگر از استادان، بزه جعل را عبارت دانسته است از: «ساختن هر چیز مثل سند به یکی از طرق پیش‌بینی شده در قانون بر خلاف حقیقت و به ضرر دیگر»^۳ تعریف دیگری که از بزه جعل بیان کرده اند عبارت از اینست که «ساختن یا تغییر دادن آگاهانه نوشته یا سایر چیزهای مذکور در قانون به ضرر دیگری به قصد جا زدن آنها به عنوان اصل»^۴ و نهایتاً برخی از اساتید حقوق جزا، جعل و تزویر را «قلب متقابلانه حقیقت در یک سند یا نوشته یا چیز دیگر به یکی از طرق مذکور در قانون به ضرر غیر» تعریف کرده‌اند.^۵ به نظر می‌رسد بهترین تعریفی را که در حقوق ایران با توجه به موارد مربوط در این مورد می‌توان ارائه داد چنین است: «جعل عبارت از ساختن یا تغییر دادن آگاهانه نوشته یا سایر چیزهای ذکر شده در قانون به قصد جازدن آنها به عنوان اصل برای استفاده خود یا دیگری و به ضرر غیر.»

۱-۳- بزه کامپیوتری (بزه رایانه ای)

تعاریف زیادی در خصوص جرایم کامپیوتری ارائه گردیده است ولی یک تعریف رسمی بین‌المللی در این خصوص وجود ندارد. تعاریف ارائه شده بیشتر جنبه کارکردی دارند و در ذیل به تعاریفی که در این خصوص از سوی مراجع ذیل ارائه گردیده است اشاره می‌کنیم:

^۱ - منصور آبادی، عباس، تقریرات درس حقوق و جزای اختصاصی، دوره کارشناسی ارشد رشته حقوق جزا و بزه شناسی، دانشگاه شیراز، سال ۱۳۸۸.

^۲ - پاد، ابراهیم، تقریرات درس حقوق جزایی اختصاصی سال ۳۵ و ۳۶ دانشگاه تهران.

^۳ - آزمایش، علی، تقریرات درس حقوق جزای اختصاصی سال ۷۵ و ۷۶ دانشگاه تهران.

^۴ - میرمحمد صادقی، حسین، حقوق کیفری اختصاصی جرائم علیه امنیت و آسایش عمومی، نشر میزان، تابستان ۱۳۸۶، ص ۲۴۷.

^۵ - سلیمانپور، محمد، جعل اسناد در حقوق ایران و از نظر حقوق تطبیقی، تهران، گنج دانش، ۱۳۴۱، ص ۱۸.



۱- سازمان همکاری و توسعه اقتصادی

«سوء استفاده از کامپیوتر شامل هر رفتار غیر قانونی، غیر اخلاقی یا غیر مجاز مربوط به پردازش اتوماتیک و انتقال داده‌ها است»^۱ ایرادی که بر این تعریف وارد است اینست که در این تعریف از واژه «سوء استفاده» از کامپیوتر به جای واژه حقوقی «بزه» استفاده شده است و شامل کلیه رفتارهای غیر قانونی، غیر مجاز و غیر اخلاقی است و این واژه‌ها دایره وسیع‌تر از مفهوم دارند. بنابراین به عنوان یک تعریف جامع و مانع قابل استفاده نمی‌باشد.

۲. کمیته اروپایی مسائل جنایی در شورای اروپا

در سال ۱۹۸۹ گزارشگری بیان کرد که در آن یکی از متخصصان چنین تعریفی ارائه کرده است: «هر فعل مثبت غیر قانونی که کامپیوتر، ابزار یا موضوع بزه باشد. یعنی به عبارت دیگر هر بزه‌ای که ابزار یا هدف آن تاثیر گذاری بر عملکرد کامپیوتر باشد» متخصص دیگری چنین تعریف کرده «سوء استفاده از کامپیوتر یعنی هر واقعه‌ای که توأم با تکنولوژی کامپیوتر شود و به واسطه آن بزه دیده متحمل خساراتی شود و مرتکب به عمد مالی یا منفعتی کسب کند یا بتواند کسب کند»^۲ نهایتاً کمیته متخصصان چنین اعلام کردند:

«مفهوم بزه کامپیوتری مشتمل بر تیپ‌های مختلف جرائمی است که اغلب بوسیله برخی دول عضو، بزه شناخته شده‌اند و برخی از دول عضو هنوز بحث قانع کننده‌ای درباره آن ارائه نکرده‌اند. به دلیل طراحی رهنمودهایی برای بزه کامپیوتری ضرورت ارائه یا گزینش تعریفی رسمی از بزه کامپیوتری بیشتر رخ می‌نماید. این امر به قانونگذاران ملی واگذار شد تا با توجه به سنن تاریخی سیستم قضایی خود، در کنار رهنمودهای کمیته تعریفی ارائه کنند که دو لیست حداقل و اختیاری را در برداشته باشد»^۳ سازمان ملل متحد در شماره ۴۴ نشریه بین‌المللی سیاست جنایی با اذعان به اینکه در زمینه جرایم کامپیوتری تعریف مورد توافقی وجود ندارد، جرایم کامپیوتری را از یک

۱ - دزیانی، محمدحسن، نشریه بین‌المللی سیاست جنایی - سازمان ملل - شماره ۴۳ و ۴۴، خبرنامه شورای عالی انفورماتیک کشور.

۲ - دزیانی، محمد حسن، ابعاد جزایی کاربرد کامپیوتر و جرایم کامپیوتری، خبرنامه انفورماتیک شماره ۵۸ شورای عالی انفورماتیک کشور - سازمان برنامه و بودجه

۳ - بزه کامپیوتری به گزارش دستاوردهای شورای اروپا به استراسبورگ ۱۹۹۰ - خرداد ماه ۱۳۷۶.



سو شامل فعالیت‌های مزهانه با ماهیت سنتی مثل سرقت و جعل دانسته که همگی معمولاً در همه جا مشمول ضمانت اجرای کیفری می‌شوند و از سوی دیگر شامل فعالیت‌های مزهانه نوینی که در آنها کامپیوتر امکان اینگونه سوء استفاده‌ها را مهیا ساخته که پیش از این امکان‌پذیر نبوده است. «در حقیقت سازمان ملل اشاره به نوعی از طبقه‌بندی جرایم کامپیوتری دارد و نه تعریف بزه کامپیوتری»^۱ نهایتاً اینکه هنوز تعریف جامعی که در سطح بین‌المللی از بزه رایانه‌ای و بزه مرتبط با رایانه مورد قبول باشد ارائه نگردیده است که ناشی از عوامل مختلفی است: «یکی از این عوامل، تفاوت سطوح کاربردی و بهره‌برداری از فن‌آوری اطلاعات در کشورهای مختلف است. عامل دیگر تفاوت در دیدگاهها و نظریات است که تعاریف بر مبنای آن قرار گرفته است. عامل بعدی تفاوت در نظام حقوق کیفری کشورهای مختلف است، که موجب می‌شود در مقابل یک پدیده نو ظهور، واکنش‌های متفاوتی از نظام‌های حقوقی مختلف بروز کند»^۲ تفاوت در تعریف جرایم رایانه‌ای موجب اختلاف در تبیین مصادیق آن شده است؛ بدین صورت که بعضی از تعاریف موسع بوده و شامل طیف گسترده‌ای از اعمال مزهانه و سوء استفاده‌های رایانه‌ای می‌شود و در مقابل، بعضی از تعاریف مضیق بود و مصادیق کمتری را در بر می‌گیرد.^۳ در حقوق ایران تعریف خاصی در مورد جرایم رایانه‌ای بیان نگردیده است و در قانون جرایم رایانه‌ای مصوب ۸۸/۳/۵ صرفاً به ارائه جرایم و مجازات‌ها پرداخت و به تعریف بزه رایانه‌ای اشاره‌ای نشده است.

گفتار سوم: رایانه - اینترنت - فضای سایبر

۱. رایانه

«کامپیوتر یا رایانه، وسیله یا دستگاهی است که می‌تواند اطلاعات و برنامه‌های کار را در حافظه‌اش نگه‌داری کند و طبق دستورات موجود در برنامه‌های مزبور اطلاعات را بپذیرد و پس از

^۱ - باستانی، برومند جرائم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری - چاپ اول ص ۲۲، ۱۳۸۳.

^۲ - بای حسینی، پور قهرمانی بابک - بررسی فقهی حقوقی جرایم رایانه‌ای چاپ اول - پاییز ۸۸ - ص ۲۴.

^۳ - خرم‌آبادی، عبدالصمد، «تاریخچه و تعریف و طبقه‌بندی جرایم رایانه‌ای» مجموعه مقالات همایش و بررسی ابعاد حقوقی فن‌آوری اطلاعات، ص ۲۷.



پردازش به صورت اطلاعات و گزارش‌های خروجی مشخص ارائه کند^۱ به عبارت دیگر، کامپیوتر ماشینی برای پذیرش داده‌ها و پردازش آنها به صورت اطلاعات مفید است. بدین ترتیب کار یک کامپیوتر شامل چهار بخش اصلی ورود، پردازش، خروج و ذخیره‌سازی داده است. از این رو چهار بخش سخت‌افزار نیز برای انجام دادن هر کدام از این اعمال لازم است که آنها را می‌توان چنین تعریف کرد:

الف - وسایل ورودی: این اجزای سخت‌افزاری، داده‌ها را دریافت کرده و به عبارتی آنها را می‌خوانند و سپس آنها را به واحد پردازش می‌فرستند.

ب - پردازش‌گر: این بخش که به آن CPU گفته می‌شود، دارای مداربندی الکترونیکی است که داده‌های ورودی را به اطلاعات درخواستی تبدیل می‌کند. CPU در حقیقت دستورات کامپیوتر را به اجرا می‌آورد.

ج - وسایل خروجی: این وسایل، داده‌های پردازش شده را برای استفاده در اختیار کاربر قرار می‌دهد.

د - وسایل ذخیره‌سازی: منظور از این وسایل همان حافظه فرعی است. این حافظه، رسانه‌های ذخیره‌سازی داده به غیر از Ram را شامل می‌شود. از جمله این رسانه‌ها می‌توان به دیسکت اشاره کرد. این وسایل، تکمیل‌کننده حافظه‌اند و می‌توانند داده‌ها و برنامه‌ها را به طور موقت نگه‌داری کنند».

۲. اینترنت

اینترنت نام مجموعه‌ای از منابع اطلاعاتی جهانی است که در سطح دنیا گسترده است. گستردگی این مجموعه به حدی است که می‌توان گفت هیچ انسانی نمی‌تواند به تنهایی تمامی اینترنت یا حتی بخشی از آن را بشناسد. «مجموعه جهانی شبکه‌ها و دروازه‌های شبکه‌ای با استفاده از "TCP/IP" همدیگر ارتباط برقرار می‌کنند. در قلب اینترنت، پشتوانه‌ای از خطوط ارتباطی سریع داده‌ها، میان گروه‌های اصلی یا کامپیوتری میزبان شامل هزاران سیستم تجاری، دولتی و آموزشی وجود

^۱ - آریا، ناصر، فرهنگ اصطلاحات کامپیوتر و شبکه‌های کامپیوتری، مرکز تحقیقات تخصصی حسابداری و حسابرسی،



دارد که داده‌ها و پیام‌ها را هدایت می‌کند.^۱ سر منشأ اینترنت به سال ۱۹۷۰ و گردهمایی شبکه‌های کامپیوتری (محلی - داخلی) باز می‌گردد. در ابتدا نام این شبکه که تحت نظر وزارت دفاع آمریکا قرار داشت **Arpanet** بود. «**Arpanet** در طول زمان دچار تغییرات بسیار شده است و در حال حاضر این شبکه اسکلت اصلی شبکه جهانی اینترنت را تشکیل می‌دهد»^۲

دسترسی به اینترنت معمولاً به چند روش صورت می‌گردد:

نخستین روش، اتصال از طریق شماره‌گیری یک تأمین کننده سرویس اینترنت با تأمین کننده سرویس‌های اطلاعاتی آماده به وسیله یک **Modem** (مودم) متصل به کامپیوتر کاربر است. این روش تنها روش به کار برده شده توسط کاربران خانگی کامپیوتر می‌باشد. روش دوم، از طریق خط اختصاصی است، مانند کاربر **TI** که به شبکه محلی، سپس کامپیوتر کاربر متصل است. این روش توسط سازمان‌های بزرگی مانند شرکتهایی که دارای گروه اختصاصی در اینترنت هستند به کار می‌رود. روش سوم نیز در حال ظهور است. در این روش کاربران از تلویزیون‌های خاصی استفاده می‌کنند. که می‌توانند فقط مستندات شبکه جهانی وب را در اختیار کاربر قرار دهد.

۳. فضای سایبر

از لحاظ لغوی در فرهنگهای مختلف «**Cyber**» به معنی مجازی و غیر ملموس و مترادف لغت انگلیسی **Virtual** می‌باشد که با توجه به گستردگی مفهوم سایبر و اطلاق آن به تمام افعال و اقدامات واقع شده در محیط شبکه‌های بین‌المللی و بی‌شمار بودن مصادیق سایبر به توصیه متخصصان و دانشمندان صاحب نام این رشته، یا فتن لغت معادل و یا ترجمه آن به زبان‌های دیگر مجاز نمی‌باشد چرا که عقیده این صاحب‌نظران با توجه به بسط مفهوم لغوی این واژه در سطح بین‌المللی، آنرا تبدیل به یک لغت بین‌المللی نموده و ترجمه آن و یا یافتن معادلی برای آن ممکن است دایره شمول و مفهوم آنرا محدود نماید لذا توصیه می‌شود لغت سایبر به یک لفظ و معنی

^۱ - اینترنت بر اساس مجموعه‌ای از شبکه‌ها که جهانی را پوشش می‌دهد ساخته شده است. این شبکه‌ها شامل انواع بسیار متفاوتی از کامپیوتر می‌باشد و بنابراین چیزی باید همه اجزا را در کنار یکدیگر نگه دارد. این وسیله IP یا TCP است. IP و TCP نام متداولی برای اتصال دهنده بین شبکه‌هایی است که تعداد آنها حداقل صد دستگاه می‌باشد.

^۲ - دزیانی محمد حسن، مقدمه cyber Law (آلمان) خبرنامه انفورماتیک، شورای عالی انفورماتیک کشور، ش ۷۱، مرداد، ۷۸، ص ۱۲۲.



مشترک بین المللی استعمال شود. به طور کلی برای وارد شدن به فضای مجازی ابزاری لازم است، از جمله کامپیوتر، مودم اتصال به شبکه بین المللی اینترنت، شبیه سازی و مجازی سازی. از مصادیق شبیه سازی می توان به کسب شخصیت یا موفقیت موهوم و خیالی یا مشابه یک شخصیت مهم توسط کاربر اشاره کرد. تمام اطلاعاتی که در اینترنت و شبکه های بین المللی وجود دارد و یا خلق می شود (اعم از واقعی یا غیر واقعی) به صورت فیزیکی و ملموس وجود ندارد و در واقع آنچه در صفحه مانیتور مشاهده می شود، موضوعات مجازی می باشند که به صورت دیجیتالی وارد شبکه شده اند. برای آنکه کاربر وارد فضای سایر از طریق شبکه اینترنت شود باید پس از فراهم آوردن تجهیزات اولیه (کامپیوتر، مودم و خطوط مخابراتی) به شبکه وصل شده و پس از آن آدرس و سایت مورد نظر خود را انتخاب کرده و با توجه به نوع، موضوع و هدف خود به بررسی و یا اقداماتی در آن بپردازد. «با توجه به این توضیحات و تعاریف ارائه شده می توان گفت که فضای سایر محیطی است مجازی و غیر ملموس که در فضای شبکه های بین المللی (که از طریق اینترنت به هم وصل می شوند) وجود دارد. در این محیط تمام اطلاعات مربوط به روابط افراد، ملت ها، فرهنگ ها، کشورها، به صورت ملموس و فیزیکی (به صورت نوشته یا تصویر، صوت و اسناد) در یک فضای مجازی و شکل دیجیتالی وجود داشته و قابل استفاده و در دسترس استفاده کنندگان و کاربران می باشد. کاربرانی که از طریق کامپیوتر، اجزای آن و شبکه های بین المللی به هم مرتبطند»^۱

۱-۴- جعل رایانه‌ای

همانگونه که در بحث مربوطه به تعریف جعل سنتی اشارت رفت با توجه به عدم تعریف بزه جعل در قوانین ایران، علمای حقوق از بزه جعل تعاریف مختلفی را بیان نموده اند. با ملاحظه تعاریف مزبور و قوانین موجود بر می آید، آنچه که تعریف شده است تعریف جعل اسناد و نوشته ها می باشد و در مورد جعل داده ها و اطلاعات کامپیوتری صراحتی ندارد. البته در حقوق برخی از کشورها از جمله انگلستان جعل بنحوی تعریف شده است که جعل داده ها و اطلاعات کامپیوتری را نیز در بر می گیرد. «به موجب بخش اول قانون «جعل و قلب سکه» (مصوب ۱۹۸۱)

^۱ - برومند باستانی، جرائم کامپیوتری و اینترنتی جلوه ای نوین از بزهکاری - چاپ اول - ۸۳ ص ۵۶.



جعل عبارت است از ساختن یک مدرک تقلبی به قصد اینکه شخص سازنده یا شخص دیگری به وسیله آن کسی را اغوا به پذیرش آن به عنوان اصل کند، تا بدین ترتیب او به ضرر خود عملی را انجام داده یا از اجرای آن سرباز زند^۱ در اینجا باید گفت که اسناد الکترونیکی و داده‌های رایانه‌ای از شمول تعاریف مربوط به جعل سنتی و در نتیجه به دلیل اصل تفسیر مضیق در امور کیفری از شمول احکام مربوط به جعل کلاسیک در قانون مجازات اسلامی خارج بوده و نمی‌توان با استفاده به این قانون جاعل رایانه‌ای را محکوم کرد. جعل رایانه‌ای تا قبل از سال ۸۲ در قوانین جزایی ایران محلی از اعراب نداشت و با تصویب قانون تجارت الکترونیکی (مصوب ۸۴/۱۰/۲۴) ماده ۶۸ این قانون به جعل کامپیوتری اختصاص یافت. ماده ۶۸ قانون مذکور بیان می‌دارد:

«هر کس در بستر مبادلات الکترونیکی از طریق ورود، تغییر، محو و توقف «داده پیام» و مداخله در پردازش «داده پیام» و سیستم‌های رایانه‌ای و یا استفاده از وسایل کاربردی سیستم‌های رمز نگاری تولید امضاء - مثل کلید اختصاصی - بدون مجوز امضاء کننده و یا تولید امضا فاقد سابقه ثبت در فهرست دفاتر اسناد الکترونیکی وی یا عدم انطباق آن وسایل با نام دارنده در فهرست مزبور و اخذ گواهی مجعول و نظایر آن اقدام به جعل داده پیام‌های دارای ارزش مالی و اثباتی نماید تا با ارایه آن به مراجع اداری، قضایی، مالی و غیره به عنوان داده پیام‌های معتبر استفاده نماید، جاعل محسوب و به مجازات حبس از یک تا سه سال و پرداخت جزای نقدی به میزان پنجاه میلیون ریال محکوم می‌شود.

تبصره: مجازات شروع به این بزه حداقل مجازات در این ماده می‌باشد.

با مذاقه در ماده و قانون فوق مشخص می‌گردد که اولاً این قانون به تعریف جعل کامپیوتری (رایانه‌ای) نمی‌پردازد بلکه مصادیق و نحوه تحقق جعل کامپیوتری را بیان می‌دارد و ثانیاً قانون مذکور خاص بوده و فقط در حدود مبادلات الکترونیکی قابلیت اجرایی دارد.

در اینجا به ذکر جعل رایانه‌ای از دیدگاه نهادهای بین‌المللی اشاره می‌کنیم.

شورای همکاری و توسعه اقتصادی (OECD) جعل رایانه‌ای را این طور تعریف کرده است:

^۱ - میرمحمد صادقی، حسین، جرائم علیه امنیت و آسایش عمومی، چاپ دوم، تهران، نشر میزان، ص ۲۴۲.



«وارد کردن، تغییر، پاک کردن، موقوف‌سازی داده‌های کامپیوتری و یا برنامه‌های کامپیوتری که به صورت عمدی و با قصد ارتکاب جعل صورت گرفته باشد.» ایراد عمده‌ای که بر این تعریف وارد است عدم ذکر شاخص‌های بزه جعل می‌باشد.

شورای اروپا تعریف زیر را از جعل رایانه‌ای ارائه نموده است:

«وارد کردن، تغییر، پاک کردن یا متوقف‌سازی داده‌هایی کامپیوتری یا برنامه‌های کامپیوتری، یا هرگونه مداخله دیگر در پردازش داده‌ها به شیوه یا تحت شرایطی، که در قوانین ملی تشریح شده است، بزه جعل را تشکیل می‌دهد، مشروط به اینکه با توجه به هدف مرسوم چنین بزه‌ی ارتکاب یافته باشد». در ماده هفتم کنوانسیون جرایم سایبر نیز جعل رایانه‌ای چنین تعریف شده است:

«هر نوع وارد کردن، تغییر، حذف یا متوقف‌سازی عمدی و بدون حق داده‌های رایانه‌ای که به ایجاد داده‌های نامعتبر منتهی می‌شود با همان قصدی که در آن انتظار می‌رود یا به کارگیری آنها در راستای هدف‌های غیر قانونی به منزله داده‌هایی که اعتبار کافی دارند اعم از آنکه داده‌ها به طور مستقیم درک شدنی و خواندنی باشند یا خیر». «جعل رایانه‌ای در واقع جعل داده‌ها می‌باشد و همانگونه که در مورد جعل اسناد سنتی عمل ارتكابی بر اسناد اثر می‌گذارد در جعل رایانه‌ای نیز عمل ارتكابی بر داده‌ها اثر می‌گذارد، با این تفاوت که داده ماهیت اسناد عادی را ندارد و اسناد عادی مکتوبند. با در دسترس قرار گرفتن دستگاههای تصویربرداری رنگی لیزری و رایانه‌ای، نسل جدیدی از تغییر و جابجایی متقلبانه و یا جعل نیز به وجود آمده است. این دستگاهها قادر به تغییر و جابجایی متقلبانه و یا جعل نیز به وجود آمده است. این دستگاهها قادر به تصویربرداری با وضوح بالا، اصلاح اسناد و حتی ایجاد اسناد جعلی بدون استفاده از نسخه اصلی آنها هستند.» ماده ۶ قانون جرائم رایانه‌ای مصوب ۱۳۸۸/۳/۵ در باب جعل رایانه‌ای اشعار می‌دارد: هر کس به طور غیرمجاز مرتکب اعمال زیر شود جاعل محسوب به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال یا هر دو مجازات محکوم خواهد شد.

الف) تغییر یا ایجاد داده‌های قابل استناد یا ایجاد یا وارد کردن متقلبانه داده به آنها



ب) تغییر داده‌ها یا علائم موجود در کارتهای حافظه یا قابل پردازش در سامانه‌های رایانه‌ای یا مخابراتی یا تراشه‌ها یا ایجاد و وارد کردن متقلبانه داده‌ها یا علائم به آنها»
با ملاحظه این ماده قانونی نیز متوجه می‌گردیم که تعریفی از جعل رایانه‌ای در قوانین ما وجود ندارد و آنچه که آمده است صرفاً ذکر مصادیق بوده ولی با توجه به قوانین مذکور می‌توان جعل رایانه‌ای را این چنین تعریف کرد:

«جعل رایانه‌ای عبارتست از ساختن یا تغییر دادن آگاهانه داده‌های رایانه‌ای یا سایر موارد مذکور در قانون دارای ارزش اثباتی به قصد جا زدن آنها به عنوان اصل برای استفاده خود یا دیگری و به ضرر غیر»

این تعریف بدواً تمام مصادیق جعل‌هایی رایانه‌ای اعم از جعل داده‌ها و جعل امضاء و سایر موارد را در بر می‌گیرد و سپس نحوه قلب حقیقت و نحوه تحقق آن به طرق مذکور در قانون منوط شده است.

۲-۱- سیر تحول تاریخی جعل رایانه‌ای

از گذشته‌های بسیار دور است که اسناد در روابط حقوقی نقش آفرینی می‌کند و نظم اسنادی مربوط به امروز نیست و از گذشته‌های دور بوده است. اما اسناد الکترونیکی یا دلایل رایانه‌ای، دلایل نوظهوری هستند که دانش بشری به نظام اثباتی و عدالت هدیه کرده است و این دلایل به صورت داده پیام در عرصه تجارت الکترونیک نمایان شده است. نظر به اینکه ادله اثبات دعوی از حیث شکل و قالب روزبه‌روز تحول چشمگیری می‌یابد و با توجه به پیشرفتهای دانش بشری در زمینه علوم رایانه‌ای باید اذعان داشت که انحصار ادله اثبات دعوی از حیث شکلی به اقرار، سند، شهادت، اماره و سوگند جوابگوی نیازهای فعلی جامعه پویا نیست و باید ادله اثبات دعوی را در قالبها و شکلهای دیگری پذیرا شد. بزه جعل به طور کلی در اکثر نظام‌های حقوقی همواره به اهمیت حفظ این بزه به عنوان یک بزه مستقل در جهت تحکیم روابط اجتماعی سالم تأکید گشته و این بزه علیرغم اینکه در بسیاری از موارد موجب بردن مال می‌شود در زمره جرائم علیه آسایش عمومی و نه جرایم علیه اموال طبقه‌بندی شده است که نشانگر توجه به ابعاد غیر مالی آن یعنی سلب اعتماد عمومی و نیز ضررهای غیر مالی دیگری است که ممکن است از ارتکاب جعل به



اشخاص وارد شود. برای مثال، جعل مدرک دانشگاهی می‌تواند باعث خدشه وارد کردن به اعتبار و حیثیت دانشگاه مورد نظر شود. «در حقوق قدیم انگلستان این بزه آنچنان شدید تلقی می‌شد که در واقع بزهی علیه اقتدار پادشاه و در نتیجه خیانت به کشور محسوب می‌گشت و مجازات اعدام را در پی داشت»^۱ هر چند که تا سال ۱۷۲۷ در این کشور فقط اسناد و مدارک رسمی و عمومی موضوع بزه جعل قرار می‌گرفتند. قدیمیترین قانون مدون بشری یعنی مجمع القوانين حمورابی در ماده ۵ خود برای قاضی در صورتی که به مخدوش کردن و از بین بردن حکم دست زند پرداخت جریمه معادل ۱۲ برابر مدعی و انفصال ابد از شغل قضا را پیش‌بینی می‌کرد. از لحاظ فقه اسلامی نیز می‌توان با استناد به عناوین کلی مثل منع اکل مال بباطل یا منع تدلیس و تقلب که در قرآن کریم به کرات مورد اشاره قرار گرفته است، ارتکاب این عمل را ممنوع و موجب عقاب و تعزیر دانست. قرآن کریم در منع «اکل مال بباطل» می‌فرماید: «یا ایها الذین آمنوا لاتاکوا اموالکم بینکم بالباطل»^۲ همینطور قرآن کریم پس از تشویق افراد به وصیت کردن به نفع اقربا و خویشاوندان عمل کسانی را که پس از شنیدن وصیت کسی آنرا به نحو تحریف شده‌ای منعکس می‌نماید تقبیح کرده است «... فمن بدلہ بعد ما سمعہ فانما اثمہ علی الذین یدلونہ ان لله سمیع علیم»^۳

۲-۱-۱- پیشینه تاریخی جعل رایانه‌ای در نظام حقوق بین الملل

بزه جعل رایانه‌ای به عنوان یکی از مهمترین جرائم رایانه‌ای به لحاظ خصیصه فراملی بودن آن همانند سایر جرائم رایانه‌ای موجب گردید اقدامات فراوانی توسط سازمانهای بین‌المللی منطقه‌ای و جهانی برای دستیابی به یک سیاست جنایی بین‌المللی ناظر بر این بزه انجام گردد. فعالیت‌های بین‌المللی برای مبارزه با این بزه در کنار سایر جرائم رایانه‌ای، از دهه ۱۹۸۰ شروع شد. سازمانهایی مانند سازمان همکاری و توسعه اقتصادی، انجمن بین‌المللی حقوق جزا، سازمان ملل متحد، اینترپول، شورای اروپا و کشورهای شرکت کننده در کنفرانس بین‌المللی مبارزه با جرائم سایبر (۲۰۰۱) بودا پست اقدامات ارزنده‌ای را در این خصوص انجام داده‌اند.

^۱ - میر محمد صادقی، حسین، حقوق کیفری اختصاصی - جرائم علیه امنیت و آسایش عمومی - ص ۲۴۰.

^۲ - آیه ۱۸۸ سوره بقره.

^۳ - آیه ۶۴ سوره نساء.



در اینجا به بررسی سابقه تاریخی بزه جعل رایانه‌ای در سازمان‌های بین‌المللی با توضیح مختصر می‌پردازیم.

۱- سازمان همکاری و توسعه (OECD)

اولین تلاش بین‌المللی در مورد تحلیل مشکلات حقوق جزا در برابر جرائم رایانه‌ای و از جمله جعل رایانه‌ای توسط سازمان همکاری اقتصادی و توسعه (OECD) صورت پذیرفت. این سازمان در سال ۱۹۷۷ شروع به ارائه رهنمودهایی در مورد حمایت از حقوق فردی و جریان بین‌المللی داده‌های شخصی کرد. از سال ۱۹۸۳ تا ۱۹۸۵ در یک کمیته تخصصی این سازمان مشغول مطالعه و بررسی راههای ممکن جهت هماهنگی بین‌المللی قوانین کیفری برای مبارزه با جرائم اقتصادی مرتبط با رایانه شد. کمیته مزبور براساس تجزیه و تحلیل تطبیقی قوانین ماهوی، فهرستی را پیشنهاد کرد و اعلام کرد که این فهرست می‌تواند به عنوان خط مشترک از سوی کشورهای عضو در نظر گرفته شده و مشمول بزه‌انگاری قرار گردند.

فهرست حداقل سوءاستفاده‌های رایانه‌ای که بر اساس پیشنهاد این سازمان باید بزه انگاری شوند شامل موارد زیر است:

۱- کلاهبرداری رایانه‌ای

۲- جعل رایانه‌ای

۳- اختلال در داده و اختلال در سیستم رایانه‌ای

۴- نقض مالکیت معنوی مربوطه به نرم‌افزارهای رایانه‌ای

۵- دستیابی یا استراق سمع در یک سیستم رایانه‌ای

همانگونه که ملاحظه کردیم به لحاظ اهمیت بزه جعل رایانه‌ای این بزه به عنوان یکی از مهمترین بزه‌هایی بوده که می‌بایست بزه انگاری می‌گشت.

۲. سازمان ملل متحد

سازمان ملل از دهه هشتاد تلاشهای خود را در خصوص مبارزه با جرائم فناوری اطلاعات شروع کرد، و نخستین بار پس از برگزاری هفتمین کنگره سازمان ملل متحد درباره پیشگیری از بزه و درمان مبهزان که در سال ۱۹۸۵ برگزار شد، دبیر کل سازمان گزارش تحت عنوان «پیشنادهای برای اقدامات هماهنگ بین‌المللی علیه اشکال به رسمیت شناخته شده جرائم در طرح اجرایی



میلان ارایه داد که در آن جرائم رایانه‌ای من جمله جعل رایانه‌ای مورد بحث قرار گرفت. پس از تشکیل کنگره هشتم سازمان ملل متحد در مورد پیشگیری از بزه و درمان میزبان (۱۹۹۰) از آن زمان به بعد به موجب قطع‌نامه این کنگره «کمیته پیشگیری و کنترل بزه» عهده‌دار سازماندهی کوشش‌های بین‌المللی برای ارتقاء و تعمیم چارچوب جامع از خطوط راهنما و استانداردهایی شد که به دولتهای عضو در برخورد با جرائم رایانه‌ای و من جمله جعل رایانه‌ای کمک کند. در کنگره نهم سازمان ملل متحد در مورد پیشگیری از بزه و درمان میزبان (۱۹۹۵) جرائم رایانه‌ای و از جمله جعل رایانه‌ای عنوان مستقل نداشته و به گروه بزه سازمان یافته فراملی تحت عنوان «چالشهای بزه فراملی و فساد» مورد توجه قرار گرفت 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 که شامل جرائم رایانه‌ای فراملی که به صورت سازمان یافته انجام می‌شوند نیز می‌گردد. در کنگره دهم سازمان ملل در مورد پیشگیری از بزه و درمان میزبان (۲۰۰۰) مجمع عمومی سازمان ملل در قطعنامه ۵۲/۹۱ مورخه ۱۲ دسامبر ۱۹۹۷ و قطعنامه ۵۳/۱۱۰ مورخه ۹ دسامبر ۱۹۹۸ در مورد تدارک برای دهمین کنگره پیشگیری از بزه و درمان میزبان سازمان ملل متحد که به وسیله شورای اجتماعی و اقتصادی پیشنهاد شده بود تصمیم گرفت به ۴ موضوع در کنگره دهم پرداخته شود که یکی از آنها جرایم مرتبط با شبکه رایانه‌ای و از جمله جعل رایانه‌ای بود. و نهایتاً به موجب بند ۱۸ بیانیه کنگره دهم از کمیسیون پیشگیری از بزه و عدالت کیفری وابسته به شورای اقتصادی اجتماعی سازمان ملل متحد دعوت به عمل آمد که با در نظر گرفتن راههای که قبلاً توسط دیگر نهادهایی بین‌المللی طی شده «توصیه‌های سیاسی» را گسترش دهد.

۳. شورای اروپا

مسئله بزه رایانه‌ای در سال ۸۶-۱۹۸۵ در برنامه کار کمیته اروپایی مشکلات ناشی از بزه، وابسته به شورای اروپا قرار گرفت. مطالعات و تحقیقات انجام شده توسط این کمیته و کمیته‌های تخصصی زیر مجموعه آن تا کنون منجر به صدور پیش‌نویس کنوانسیون جرایم سایبر و چندین توصیه‌نامه به شرح زیر گردیده است:



توصیه نامه شماره ۹ - توصیه نامه شماره ۱۳ - توصیه نامه شماره ۱۰ - توصیه نامه شماره ۱۵ -
توصیه نامه شماره ۴ - توصیه نامه شماره ۱۰ - پیش‌نویس کنوانسیون جرایم سایبر - توصیه نامه
شماره ۲ - پروتکل الحاقی به کنوانسیون جرایم سایبر در خصوص بزه‌انگاری اعمال دارای
ماهیت نژاد پرستانه و بیگانه ستیزانه.

و به لحاظ اهمیت توصیه نامه‌های شماره ۹ و شماره ۱۳ مختصر به آنها اشاره می‌کنیم.

الف- توصیه نامه شماره ۹ (۸۹) R شورای اروپا در مورد بزه رایانه‌ای، ۱۳ دسامبر ۱۹۸۹
این توصیه نامه حاوی ۵ فصل و ۳ ضمیمه می‌باشد. در فصل اول ملاحظه کلی از جمله مربوط
به سیاست جنایی، در فصل دوم دو فهرست اجباری و اختیاری از جرائم رایانه‌ای، در فصل سوم
مشکلات مربوطه آئین دادرسی، در فصل چهارم جنبه‌های بین‌المللی در فصل پنجم دیگر جنبه‌های
بزه رایانه‌ای ذکر شده است. منظور از فهرست اجباری فهرست آن دسته از جرائم فناوری اطلاعات
است که نظام حقوقی همه کشورهای عضو شورای اروپا در سال ۱۹۸۹ اجماع بر بزه‌انگاری آنها
داشته‌اند و شامل ۸ عنوان میزبانه به شرح زیر است:

۱- کلاهبرداری رایانه‌ای

۲- جعل رایانه‌ای

۳- تخریب داده‌ها یا برنامه‌های رایانه‌ای

۴- اختلال در عملکرد سیستم رایانه‌ای

۵- دستیابی بدون حق

۶- شنود بدون حق

۷- ارائه و ایجاد مجدد و من غیر حق یک برنامه رایانه‌ای حمایت شده

۸- ارائه و ایجاد مجدد یک توپوگرافی

همانگونه که بیان گردید به لحاظ اهمیت موضوع بزه، جعل رایانه‌ای به عنوان یکی از جرائم
فناوری اطلاعات می‌باشد که در فهرست اجباری قید گردیده است.

ب - توصیه نامه شماره ۱۳ (۹۵) R ناظر به مشکلات آئین دادرسی کیفری مرتبط با فناوری
اطلاعات موضوع این توصیه نامه اصول و قواعد مربوط به آئین دادرسی کیفری جرائم فن‌آوری
اطلاعات و از جمله جعل رایانه‌ای می‌باشد.



این توصیه نامه حاوی ۷ فصل بحث عناوین زیر است:

۱- نقیثش و توقیف

۲- مراقبت فنی

۳- تعهد برای همکاری با مقامات تحقیق

۴- ادله الکترونیکی

۵- استفاده از رمزنگاری

۶- تحقیق، آمار و آموزش

۷- همکاری بین‌المللی

۴- کنوانسیون جرایم سایبر

این کنوانسیون در بردارنده ابعاد مختلف جرایم سایبری از حیث حقوق جزای ماهوی، حقوق جزای شکلی و حقوق جزای بین‌المللی می‌باشد. کنوانسیون مذکور حاوی ۴ فصل تحت عناوین ذیل است:

فصل یکم، راجع به کاربرد اصطلاحات است. فصل دوم مربوط به تدابیری است که در سطح ملی باید رعایت شود. فصل سوم، در خصوص همکاری بین‌المللی است و فصل چهارم در مورد مقررات نهایی است. بخش اول فصل دوم کنوانسیون در بردارنده حقوق جزای ماهوی است، در این بخش به عناصر مادی و معنوی ۹ عنوان کلی مبزهانه اشاره گردیده است و از کشورها خواسته شده است نسبت به بزه‌انگاری آنها اقدام نمایند. هر یک از این جرائم خود دارای شقوقی هستند. از جمله این جرائم می‌توان به جعل مرتبط با رایانه اشاره کرد که ذیل شق جرائم مرتبط با رایانه قلمداد می‌گردد. علیهذا با توجه به اهمیت بزه جعل رایانه‌ای نیز در زمره جرائم مهم مرتبط با رایانه که در کنوانسیون سایبر قلمداد گردیده است.

۵. پروتکل الحاقی به کنوانسیون جرایم سایبر در خصوص بزه‌انگاری اعمال نژادپرستانه و ضد بیگانه (مصوبه ۷ نوامبر ۲۰۰۲ استراسبورگ)

اهداف پروتکل هماهنگ کردن قوانین ماهوی در مقابله با نژادپرستی و بیگانه ستیزی در اینترنت و بهبود همکاری‌های بین‌المللی در این خصوص می‌باشد که از موضوع بحث ما خارج می‌باشد.

۶. انجمن بین‌المللی حقوق جزا



انجمن بین‌المللی حقوق جزا یک سازمان غیر دولتی است که همکاری فعالی با سازمان ملل دارد. در سال ۱۹۹۰ یکی از موضوعاتی که انجمن مطرح کرد جرائم رایانه‌ای و سایر جرائم فناوری اطلاعات بود. انجمن بین‌المللی حقوق جزا در نشست سال ۱۹۹۲ خود در ورتسبورگ آلمان، فهرست‌های حداقل و اختیاری شورای اروپا را به عنوان مصادیق پذیرفته شده بزه رایانه‌ای تأیید کرد و در نشست ۱۹۹۴ خود در ریودوژانیرو و ضمن تأکید مجدد به فهرست‌های مزبور از جرائم زیر نیز به عنوان بزه رایانه‌ای نام برد:

۱- قاچاق کلمات رمز

۲- انتشار ویروس یا برنامه‌های مشابه

۳- دستیابی به اسرار خلاف واقع

۴- به کارگیری، انتقال و دگرگونی داده شخصی

که ملاحظه می‌گردد دگرگونی داده‌های شخصی در واقع از مصادیق جعل رایانه‌ای می‌باشد که در اینجا بزه‌نگاری گردیده است.

۷. سازمان پلیس بین‌المللی (اینترپول)

اینترپول از جمله سازمان‌های بین‌المللی است که در برخورد با جرائم مرتبط با فن‌آوری اطلاعات نقش عمده‌ای داشته است. «گروه‌های کاری منطقه‌ای در اروپا، آسیا، آمریکا و آفریقا مشغول به کارند و زیر نظر کمیته راهبردی جرائم فن‌آوری اطلاعات مستقر در دبیرخانه کل اینترپول فعالیت می‌نمایند.»^۱ اولین کنفرانس بین‌الملل بزه رایانه‌ای توسط اینترپول در ۱۹ و ۲۰ آوریل ۱۹۹۵ در لیون با حضور نمایندگان پلیس بین‌الملل دولتها تشکیل گردید و مسائل مربوط به طرق ارتکاب جرائم رایانه‌ای و از جمله جعل رایانه‌ای و تکنولوژیهای در اختیار برای کشف و پی‌جویی و جمع‌آوری ادله در این جرائم و قوانین موجود مورد بررسی قرار گرفت و نهایتاً توصیه نامه‌ای را به تصویب رساند. در این توصیه نامه با توجه به اهمیت فزاینده استفاده و سوءاستفاده از رایانه در همه انواع جرائم و از جمله جعل، اعلام شد که پلیس بین‌الملل کارهایی را در جهت

^۱ - کمیته مطالعات حقوق تکنولوژی، آشنایی با پلیس جنایی بین‌المللی، خبرنامه حقوق فناوری، دفتر همکاریهای فناوری ریاست جمهوری، شماره ۸، ص ۳۱، ۱۳۸۲.



مبارزه با جرائم رایانه‌ای انجام داده است که توسط کشورهای عضو با ید مورد توجه قرار گیرند. برخی از این کارها عبارتند از:

- ۱- برقراری نقاط ارجاع مرکزی ملی و اجرا و بکارگیری پیام بزه رایانه‌ای برای انجام تبادل اطلاعات در موارد مزبور
- ۲- انتشار کتابی در زمینه رایانه‌ها و بزه و ارائه کتابچه جامع بزه رایانه‌ای در آینده نزدیک
- ۳- آماده کردن رشته‌های آموزشی برای تحقیق کنندگان پلیس.

۱-۶- پیشینه تاریخی جعل رایانه‌ای در حقوق جزای ایران

رایانه از اوایل سال ۱۳۴۰ یعنی حدود ۲۲ سال پس از اختراع اولین رایانه وارد ایران شد. بانک ملی و شرکت نفت، از جمله نهادهایی بودند که کار با رایانه را در سال ۱۳۴۱ شروع کردند. تعداد رایانه‌های ایران در سال ۱۳۴۵ جمعاً نه رایانه بود و در سال ۱۳۴۹ به ۷۸ دستگاه رسید. با سیاست‌گذاری و فعالیت نهادهای متولی فن‌آوری اطلاعات و تلاش و سرمایه‌گذاری بخش خصوصی، فن‌آوری اطلاعات در سالهای اخیر رشد نسبتاً خوبی داشته است. 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 وبسایت‌ها و وبلاگ‌ها به انتشار افکار و اندیشه‌ها و مطالب علمی، سیاسی، اقتصادی و اجتماعی، فرهنگی و مذهبی خود بپردازند. در مورد تاریخچه بزه رایانه‌ای در ایران باید خاطر نشان ساخت که با توجه به اینکه کارایی و استفاده از رایانه از ابتدای ورود آن تا دهه ۱۳۷۰ محدود بوده است، در نتیجه این بزه سابقه چندانی در کشور ما ندارد و چنانچه بزه احتمالی در این خصوص واقع شده باشد گزارشی از آن منتشر نگردیده است. وقوع بزه رایانه‌ای به تدریج از دهه ۱۳۷۰ در ایران شروع شد. «سوءاستفاده از رایانه برای اتکاب جرایم سنتی، به کارگیری ویروس از طریق توزیع حامل‌های داده آلوده به ویروس، سوءاستفاده مالی و تکثیر غیر مجاز نرم‌افزارهای رایانه‌ای از جمله جرایم رایانه‌ای هستند که در مقیاس بسیار کم در دهه ۱۳۷۰ واقع شده و با قوانین کیفری مرسوم مورد رسیدگی قرار



گرفته‌اند.^۱ قانون حمایت از مؤلفان را می‌توان اولین واکنش تقنینی ایران در مورد جرایم رایانه‌ای دانست. دومین واکنش تقنینی ایران که به نوعی درباره جرایم رایانه‌ای «قانون ترجمه یا تکثیر کتب و نشریات و آثار صوتی (مصوب ۱۳۵۲/۱۰/۶) است. از نیمه دوم دهه ۱۳۷۰ و به ویژه از ابتدای دهه ۱۳۸۰ که استفاده از رایانه‌های شخصی توسط سازمانهای اداری و مؤسسات خصوصی و افراد حقیقی گسترش یافته و دسترسی به خدمات متعدد اینترنت امکان‌پذیر شده، ارتکاب جرایم رایانه‌ای نیز رشد نسبتاً سریعی داشته است. اشاعه فحشا و منکرات و انتشار عکس‌ها و تصاویر و مطالب خلاف عفت عمومی، ایجاد اختلاف بین اقشار جامعه از طریق طرح مسایل قومی و نژادی، انتشار مطالب نژاد پرستانه، انتشار اسناد و وسایل محرمانه، اهانت به مقدسات مذهبی و دینی، اهانت و افترا به مقامات دولتی و اشخاص حقیقی و حقوقی، سرقت ادبی و غیره از جمله جرایمی‌اند که بعد از فراهم شدن امکان استفاده از خدمات اینترنت از طریق وب‌سایت‌ها و وبلاگ‌ها، پست الکترونیک، گروه‌ها خبری، چت و سایر سرویسهای اینترنت به وقوع پیوسته‌اند. قانونگذار در سال ۱۳۷۹ در برابر برخی جرایم رایانه‌ای واکنش نشان داده و با الحاق تبصره سوم به ماده اول قانون مطبوعات مقرر داشت: «کلیه نشریات الکترونیکی مشمول مواد این قانون است.» پس سومین واکنش قانونی کشور ما در برابر بعضی از جرایم رایانه‌ای قانون اصلاح مطبوعات مصوب ۷۹/۱/۳۰ مجلس شورای اسلامی است که در تاریخ ۷۹/۲/۷ مورد تأیید شورای نگهبان قرار گرفته است. چهارمین واکنش قانونی کشور ما در مقابل جرایم رایانه‌ای از طریق وضع «قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای» به عمل آمد. این قانون در تاریخ ۷۹/۱۰/۴ به تصویب مجلس شورای اسلامی و در تاریخ ۷۹/۱۰/۱۰ به تأیید شورای نگهبان رسیده است. ماده ۱۳ قانون مذکور نقض حقوق پدیدآورندگان آن دسته از نرم‌افزارهای رایانه‌ای را که مورد حمایت این قانون قرار گرفته‌اند، بزه تلقی و برای آن مجازاتی معادل ۹۱ روز تا شش ماه حبس و جزای نقدی تعیین کرده است. موارد نقض حقوق مورد حمایت این قانون ممکن است به شکل استفاده غیرمجاز، کپی‌برداری غیرمجاز، تکثیر یا توزیع و یا هر عملی باشد که منجر به تعرض به حقوقی

^۱ - حسینعلی بای، بابک پور قهرمانی، بررسی فقهی حقوقی جرایم رایانه‌ای، پژوهشگاه علوم و فرهنگ اسلامی - چاپ اول



مادی و معنوی پدیدآورندگان این آثار می‌شود. آنچه از سابقه تاریخی جرایم رایانه‌ای تا کنون برشمرده‌ایم مرتبط با جرائم خاص رایانه‌ای راجع به موضوع در نظر گرفته در قانون مزبور می‌باشد و قوانین مذکور در خصوص جعل رایانه‌ای ساکت بوده است و هیچگونه اشاره بدان ننموده‌اند ولی موارد ذیل بالصرّاحه در خصوص جعل رایانه‌ای پرداخته‌اند و دلالت بر سابقه جعل رایانه‌ای در حقوق ایران می‌نماید. پنجمین عکس‌العمل قانون‌گذار در ایران در مقابل جرایم رایانه‌ای و اولین واکنش آن در قبال بزه رایانه‌ای در سال ۱۳۸۲ از طریق تصویب قانون مجازات جرایم نیروهای مسلح مصوب ۸۲/۱۰/۹ مجلس شورای اسلامی به عمل آمد. به موجب ماده ۱۳۱ این قانون جعل اطلاعات و داده‌های رایانه‌ای تسلیم و افشای غیرمجاز اطلاعات و داده‌ها به افرادی که صلاحیت دسترسی به آن‌را ندارد، سرقت و یا تخریب حامل‌های داده و سوءاستفاده مالی از طریق رایانه (کلاهبرداری و اختلاس) توسط نظامیان بزه تلقی و مرتکب حسب مورد به مجازات بزه ارتكابی محکوم می‌شود. به موجب قسمت اول ماده ۱۳۱ قانون مجازات جرایم نیروهای مسلح: «هرگونه تغییر یا حذف اطلاعات، الحاق یا تقدیم یا تأخیر تاریخ نسبت به تاریخ حقیقی و نظایر آن که به طور غیر مجاز توسط نظامیان در سیستم رایانه‌ای و نرم‌افزارهای مربوطه صورت گیرد بزه محسوب می‌شود و حسب مورد مشمول مجازات مندرج در مواد مربوط به این قانون می‌باشند.

فصل دوم: بررسی و تحلیل مبانی و عناصر تشکیل دهنده جعل رایانه‌ای

۲-۱- سیر تحول تاریخی جعل رایانه‌ای

«ماده ۱۳۱ قانون مجازات جرایم نیروهای مسلح برای اولین بار در ایران داده‌های رایانه‌ای را به عنوان موضوع جعل مطرح نموده و جعل رایانه‌ای را بزه‌انگاری کرده است. ششمین واکنش قانونی مرتبط با جرایم رایانه‌ای و دومین واکنش آن در قبال جعل رایانه‌ای از طریق تصویب قانون تجارت الکترونیکی مصوب ۸۲/۱۰/۱۷ مجلس شورای اسلامی به عمل آمده است. به موجب مواد ۷۷، ۶۷، ۶۸، ۶۹، ۷۴، ۷۵، ۷۶ این قانون کلاهبرداری، جعل و دستیابی و افشاء غیرمجاز اسرار تجاری نقض حقوق مربوط به مالکیت معنوی (کپی رایت) و غیره که از طریق رایانه در بستر تجارت الکترونیکی انجام شود بزه تلقی و برای آن مجازات تعیین گردیده است. بزه جعل رایانه‌ای در ماده ۶۸ قانون تجارت الکترونیکی پیش‌بینی شده است. بر پایه این ماده «هر کس در بستر مبادلات



الکترونیکی از طریق ورود، تغییر، محو و توقف داده پیام و مداخله در پردازش داده پیام و سیستم‌های رایانه‌ای و یا استفاده از وسایل کاربردی سیستم‌های رمزنگاری تولید امضاء مثل کلید اختصاصی بدون مجوز امضاء کننده و یا تولید امضای فاقد سابقه ثبت در فهرست دفاتر اسناد الکترونیکی و یا عدم انطباق آن وسایل با نام دارنده در فهرست مزبور و اخذ گواهی مجعول و نظایر آن اقدام به جعل داده پیام‌های دارای ارزش مالی و اثباتی نماید تا با ارائه آن به مراجع اداری، قضایی، مالی و غیره به عنوان داده پیام‌های معتبر استفاده نماید جعل محسوب و به مجازات حبس از یک تا سه سال و پرداخت جزای نقدی به میزان پنجاه میلیون ریال محکوم می‌شود.

تبصره - مجازات شروع به این بزه حداقل مجازات در این ماده می‌باشد.

هفتمین واکنش قانونی مرتبط با جرایم رایانه‌ای و سومین واکنش آن در برابر بزه جعل رایانه‌ای تصویب قانون جرایم رایانه‌ای مصوب ۱۳۸۸/۳/۵ مجلس شورای اسلامی بوده است. و قانونگذار با تصویب این قانون برای اولین بار دست به نوعی بزه‌انگاری و اعمال مجازات نمود که به صورت عام و کلی و نه در بستر خاص خود وارد نظام حقوقی ایران گردیده، توضیح مطلب آنکه هر یک از قوانین فوق‌الذکر در بستر خاص خود قابلیت اعمال دارند. مثلاً قانون مطبوعات صرفاً نسبت به جرایم رایانه‌ای ارتكابی در قالب نشریات الکترونیکی و قانون مجازات جرایم نیروهای مسلح صرفاً در مورد بعضی از جرائم رایانه‌ای نظامیان و قانون تجارت الکترونیکی فقط در مورد برخی از جرایم رایانه‌ای ارتكابی در بستر تجارت الکترونیکی قابل اجرا هستند حال آنکه قانون جرایم رایانه‌ای بصورت کلی و عام الشمول می‌باشد که به اعتبار خاصی قابلیت اعمال ندارد. ماده ۶ این قانون در باب جعل رایانه‌ای که اشعار می‌دارد: «هر کس به طور غیرمجاز مرتکب اعمال زیر شود جعل محسوب و به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال یا هر دو مجازات محکوم خواهد شد.

الف) تغییر یا ایجاد داده‌های قابل استناد یا ایجاد یا وارد کردن متقلبانه داده به آنها

ب) تغییر داده‌ها یا علائم موجود در کارتهای حافظه یا قابل پردازش در سامانه‌های رایانه‌ای یا مخابراتی یا تراشه‌ها یا ایجاد و وارد کردن متقلبانه داده‌ها یا علائم به آنها.»

آنچه در باب سابقه تاریخی جعل رایانه‌ای در حقوق جزای ایران وجود دارد. همان است که بر شمرديم ولی از آنجا که سیستم‌های رو به رشد کامپیوتری فرصت‌های تازه و بسیار پیشرفته‌ای را



برای قانون‌شکنی در اختیار مجریان گذارده و توان بالقوه ارتکاب گونه‌های مرسوم جرایم را به شیوه‌های غیر مرسوم به وجود می‌آورند و در واقع بزه رایانه‌ای تهدیدی مهم علیه جامعه اطلاعاتی تبدیل شده است لذا نظام‌های قانونگذاری و حقوقی باید سیر خود را به سمت و سوی سوق دهند که توجه عمده‌ای به جرایم رایانه‌ای داشته باشند. در واقع کلیه خلأهای قانونی در این مسیر برداشته شود زیرا جوامع در واقع از سمت جرایم سنتی به سمت جرائم رایانه‌ای در پیش هستند.

۲-۲- مبانی بزه‌انگاری جعل رایانه‌ای

با فراگیر شدن و استفاده از رایانه و نرم‌افزارهای رایانه‌ای در عرصه‌های مختلف زندگی، حافظه رایانه و نرم‌افزارها جایگزین سند و نوشته سنتی میشود و در سطح گسترده‌ای برای بیان و اعلام اراده از رایانه استفاده خواهد شد. در بادی امر به نظر می‌رسد تفاوتی بین فضای مجازی (سایبری) با فضای حقیقی در تحقق یا فتن بزه جعل و در نهایت مبنای بزه‌انگاری آن وجود ندارد ولی باید خاطر نشان ساخت که عنوان جزایی جعل سنتی اقدام علیه داده‌های رایانه‌ای را در بر نمی‌گیرد و با حمایت از این داده‌ها نیازمند بزه‌انگاری مستقل می‌باشیم و با توجه به تمایزهایی که در رفتار و شرایط و اجزای آن (رکن مادی) در فضای سایبری وجود دارد، به نظر می‌رسد ناچار خواهیم بود که قوانین ویژه‌ای برای این فضا در نظر بگیریم. به ویژه که در چنین مسائلی فرایند ارتکاب بزه متفاوت بوده و مسؤولیت‌های ناشی از آن می‌تواند متفاوت باشد و قوانین را چون نمی‌توان بدین حد وسیع تفسیر کرد که شامل این موارد شود برخی از عنوان‌ها قانون خاص می‌خواهد:

زندگی در اجتماع توأم با سود و زیان است و زیان‌هایی که در روابط اجتماعی از رفتارهای ما ناشی می‌شود دو دسته‌اند:

۱- زیان‌های قابل تحمل

۲- زیان‌های غیر قابل تحمل

زیان‌های قابل تحمل که خیلی به آن بهاء نمی‌دهیم و در مقابل جبران بر نمی‌آییم و مستلزم هیچ واکنشی نیست ولی زیان‌های غیر قابل تحمل می‌بایست جبران شود و افراد نمی‌توانند آن‌را نادیده بگیرند و دو بخش می‌باشد:

۱- زیان‌های غیر قابل تحمل شدید ۲- زیان‌های غیر قابل تحمل غیر شدید



اگر زیان غیر قابل تحمل و شدید نبود واکنش غیر کیفری داریم مثلاً می‌توان به تمسک به باب مسؤولیت مدنی در جهت جبران ضرر و زیان برآیم ولی اگر زیان و ضرر موضوع بحث به صورت غیر قابل تحمل و شدید باشد در اینجا مستلزم واکنش کیفری می‌باشیم که ما آن را منع می‌کنیم که چنین زیانی وارد نشود. در بحث جعل و تزویر و همچنین جعل رایانه‌ای می‌گوئیم که سند یا حافظه رایانه و نظم اسنادی به عنوان یک ارزش در نظام حقوقی ما می‌باشد و از ارزش و اعتبار برخوردار است و بر همین اساس رفتارهایی که مخالف با نظم اسنادی هستند، رفتارهایی است که زیان شدید و غیر قابل تحمل را ایجاد می‌کند و نظم اسنادی را مخدوش می‌سازد. جعل و تزویر جهت حفظ و حمایت آن و جلوگیری از زیانهای شدید که به چنین اسنادی که با ارزش هستند وارد می‌شود و به همین خاطر بزه‌نگاری شده است. «استحکام روابط اجتماعی، اقتصادی و غیره منوط به آن است که افراد جامعه بتوانند به صحت و اصالت اسناد الکترونیکی و داده‌های رایانه‌ای که برای اهداف مختلف در اختیار آن‌ها است و یا بین آنها مبادله شده و مورد اشاره قرار می‌گیرند اطمینان داشته باشند و از اینرو است که این پیشنهاد که چون جعل در واقع مقدمه‌ای برای استفاده بعدی از سند مجعول یا برای ارتکاب کلاهبرداری و نظایر آن‌ها و بنابراین نباید بزه مستقلی محسوب شود بلکه جز در موارد استثنایی مثل جعل اسکناس و قلب سکه، فرد مرتکب را تنها باید در صورت «مورد استفاده قرار دادن» سند مجعول یا ارتکاب «کلاهبرداری» و یا در صورت امکان، تحت عنوان شروع به کلاهبرداری به محاکمه کشید. در اکثر نظامهای کیفری موجود دنیا پذیرفته نشده است.^۱ برعکس در این نظام‌ها همواره به اهمیت حفظ این بزه به عنوان یک بزه مستقل در جهت تحکیم روابط اجتماعی سالم تأکید گشته است.^۲ «این بزه علی‌رغم این که در بسیاری از موارد موجب بردن مال می‌شود، در زمره جرائم علیه آسایش عمومی و نه جرایم علیه اموال طبقه بندی شده است که نشانگر توجه به ابعاد غیر مالی آن، یعنی سلب اعتماد عمومی و نیز ضررهای

۱- see for example *criew* [۱۹۷۰] crim LR ۵۸۴ and *Gla³ ebrook* [۱۹۷۰] crim LR ۵۵۴, cited in *smith and Hogan. Criminal Law* [London: Butter worths ۷th ed. ۱۹۹۲] p.۵۶۸ G. Williams, *forgery and falsity*[۱۹۷۴ crim. L.R.۷۱

^۲ -see:uk., the Law commission Reportion *forgery and counterfeit currency* (No.۵۵ ۱۹۷۳) Para ۴۲ and chapter ۳ of discussion paper of model criminal code officers committee of the standing committee of Attorneys General (Australia: july ۱۹۹۴ p.۲۳)



غیر مالی دیگری است که ممکن است از ارتکاب جعل به اشخاص وارد شود.^۱ بنابراین در گذشته اعلام و بیان اراده و بیشتر موارد به صورت مستقیم و شفاهی صورت می‌پذیرفت ولی در حال حاضر در سطح گسترده‌ای از وسایلی همانند سند و نوشته برای این منظور استفاده می‌شود به همین خاطر در جهت برقراری روابط حقوقی و اثبات و تثبیت موقعیتهای حقوقی، حل و فصل اختلافات و استفاده از حقوق و امتیازات گوناگون فردی و اجتماعی، اسناد و نوشتجات نقش مهم و اساسی را در دنیای امروز ایفا می‌کنند. به همین اساس امروزه کمتر رابطه و موقعیت حقوقی وجود دارد که به سند و نوشته وابسته نباشد. مبنای بزه‌انگاری جعل و تزویر نیز در همین امر نهفته است که نظم حقوقی در سطوح مختلف به وسیله سند و نوشته بر قرار می‌شود و در صورتیکه اقداماتی بر روی اسناد و نوشتجات انجام شود که منجر به بی‌اعتباری آنها گردد. به نظم حقوقی خدشه و لطمه وارد خواهد شد. از این رو در جهت حمایت از موقعیتهای گوناگون حقوقی قانونگذار ساختن و یا مخدوش کردن سند و نوشته و اشیای مشابه با آنها را بزه و قابل مجازات دانسته است و در فضای سایبری نیز حافظه رایانه و نرم‌افزار نیز می‌تواند موضوع جعل و تزویر قرار گیرد چه آنکه داده‌های قابل استناد و یا داده‌ها و علائم موجود در کارتهای حافظه و قابل پردازش در سامانه‌های رایانه‌ای یا مخابراتی و تراشه که در واقع موضوعات جعل رایانه‌ای را تشکیل می‌دهند قابلیت تحقق موقعیتهای حقوقی و ایجاد روابط حقوقی و به نوعی اعلام و بیان اراده را تشکیل می‌دهند که هرگونه تغییر یا ایجاد آنها و وارد کردن متقلبا نه داده به آنها در واقع اقدامی مخل نظم حقوقی بوده و چون نوعی از بزه جعل را تحقق می‌بخشد، شایسته است که از ضمانت اجرای کیفری برخوردار باشد، به تعبیر دیگر از حیث مبنای بزه‌انگاری تفاوتی بین جعل سنتی و جعل رایانه‌ای وجود ندارد و هر دو در نظم حقوقی اخلال ایجاد می‌کنند.

۲-۳- عناصر متشکله بزه جعل رایانه‌ای

در این فصل به ارکان بزه جعل رایانه‌ای و شرایط ماهوی آن و همچنین رفتار مزه‌خانه و شرایط تحقیق می‌پردازیم و در جریان بررسی موارد فوق به ارکان بزه جعل رایانه‌ای موضوع ماده ۶ قانون

^۱ - میرمحمد صادقی، حسین - حقوق کیفری اختصاصی - جرایم علیه امنیت و آسایش عمومی - چاپ هشتم - تابستان ۸۶ ص ۲۴۰.



جرایم رایانه‌ای و ماده ۱۳۱ قانون مجازات جرائم نیروهای مسلح و ماده ۶۸ قانون تجارت الکترونیکی و ماده ۷ کنوانسیون جرائم سایبر از حیث مطالعه تطبیقی ورود می‌کنیم. این فصل متشکل از سه مبحث می‌باشد. در مبحث اول به رکن قانونی بزه جعل رایانه‌ای نظر داریم و مبادرت به ذکر قوانین داخلی راجع به جعل رایانه‌ای می‌نماییم. در مبحث دوم، رکن مادی بزه جعل رایانه‌ای را مورد بررسی قرار می‌دهیم. این مبحث متشکل از پنج گفتار می‌باشد که عبارتند از: نحوه و شرایط رفتار مرتکب، موضوع بزه، وسیله ارتکاب بزه، نتیجه حاصل از بزه و مرتکب بزه و خصوصیت مرتکب. در هر گفتار سعی بر آن گردیده است که جعل رایانه‌ای موضوع قوانین فوق‌الذکر را از حیث هر گفتار مورد تجزیه و تحلیل قرار داده و معمولاً توأم با دیدگاه انتقادی نیز می‌باشد. در مبحث سوم به رکن معنوی بزه جعل رایانه‌ای و مطالب مرتبط با آن می‌پردازیم.

۲-۳-۱- رکن قانونی

برای بزه قلمداد کردن یک عمل، ذکر ممنوعیت و بیان حرمت آن به همراه وضع ضمانت اجرای مناسب توسط مقنن ضروری می‌باشد. در خصوص جعل سنتی ماده ۵۲۳ و مواد بعدی آن در قانون مجازات اسلامی مصوب ۱۳۷۵، به انضمام دیگر مواد مربوط به جعل که در قوانین متفرقه پیش‌بینی شده و نیز آرای وحدت رویه دیوانعالی کشور، اجزای قانونی بزه جعل را تشکیل می‌دهند. در خصوص بزه جعل رایانه‌ای نخست باید به این نکته اشاره شود که به دلیل اصل لزوم تفسیر مضیق قوانین کیفری نمی‌توان با استناد به مواد عام راجع به جعل سنتی ذکر گردیده در قانون مجازات اسلامی، داده‌ها و اسناد رایانه‌ای را موضوع این بزه بر شمرد و مرتکب جعل رایانه‌ای را به راجع به جعل رایانه‌ای در حقوق جزای ایران می‌باشیم. و همانگونه که در فصل تمهیداتی و در مبحث سابقه تاریخی بزه جعل رایانه‌ای اشارت گردید در حقوق جزای ایران به لحاظ نوظهور بودن بزه جعل رایانه‌ای ما فقط با سه قانون کیفری مواجه می‌باشیم که فی‌الواقع رکن قانونی بزه جعل رایانه‌ای را تشکیل می‌دهد و قانونگذار ایران با بزه‌انگاری این عنوان جزایی در سه قانون کیفری مبادرت به تعیین ضمانت اجرای کیفری نموده است که صرفاً به بیان مواد قانونی مربوط به جعل رایانه‌ای در این فصل بسنده می‌کنیم.



۱- به موجب ماده ۶ قانون جرایم رایانه‌ای مصوب ۸۸/۳/۵ مجلس شورای اسلامی «هر کسی به طور غیرمجاز مرتکب اعمال زیر شود جاعل محسوب و به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال یا هر دو مجازات محکوم خواهد شد.

الف) تغییر یا ایجاد داده‌های قابل استناد یا ایجاد یا وارد کردن متقلبانه داده به آنها

ب) تغییر داده‌ها یا علائم موجود در کارتهای حافظه یا قابل پردازش در سامانه‌های رایانه‌ای یا مخابراتی یا تراشه‌ها یا ایجاد و وارد کردن متقلبانه داده‌ها یا علائم به آنها.»

۲- به موجب ماده ۶۸ قانون تجارت الکترونیکی^۱ مصوب ۸۲/۱۰/۱۷ که نخستین قانون در ایران در زمینه‌ی بزه‌های مربوط به فناوری اطلاعات و شاخه‌ی خاص آن یعنی بزه‌های مربوط به تجارت الکترونیکی است «هرکس در بستر مبادلات الکترونیکی از طریق ورود، تغییر، محو و توقف داده پیام و مداخله در پردازش داده پیام و سیستم‌های رایانه‌ای و یا استفاده از وسایل کاربری سیستم‌های رمزنگاری تولید امضاء مثل کلید اختصاصی بدون مجوز امضاء کننده و یا تولید امضاء فاقد سابقه ثبت در فهرست دفاتر اسناد الکترونیکی و یا عدم انطباق آن وسایل با نام دارنده در فهرست مزبور و اخذ گواهی مجعول و نظایر آن اقدام به جعل داده پیام‌های دارای ارزش مالی و اثباتی نماید تا با ارائه آن به مراجع اداری، قضایی، مالی و غیره به عنوان داده پیام‌های معتبر استفاده نماید جاعل محسوب و به مجازات حبس از یک تا سه سال و پرداخت جزای نقدی به میزان پنجاه میلیون ریال محکوم می‌شود. تبصره: مجازات شروع به این بزه حداقل مجازات در این ماده می‌باشد.»

۳- به موجب ماده ۱۳۱ قانون مجازات جرائم نیروهای مسلح مصوب ۸۲/۱۰/۹ مجلس شورای اسلامی «هرگونه تغییر یا حذف اطلاعات، الحاق، تقدیم یا تأخیر تاریخ نسبت به تاریخ حقیقی و نظایر آن که به طور غیرمجاز توسط نظامیان در سیستم رایانه و نرم‌افزارهای مربوطه صورت می‌گیرد و همچنین اقداماتی از قبیل تسلیم اطلاعات طبقه‌بندی شده‌ی رایانه‌ای به دشمن یا افرادی که صلاحیت دسترسی به آن دی یا دیسک‌های حاوی اطلاعات یا معدوم کردن آنها یا سوءاس اطلاعات را ندارند، افشاء غیرمجاز اطلاعات، سرقت اشیاء دارای ارزش اطلاعاتی مانند سی‌فاده‌های مالی که نظامیان به وسیله رایانه مرتکب می‌شوند، بزه محسوب و حسب مورد مشمول



مجازات‌های مندرج در مواد مربوط به این قانون می‌باشند. ماده ۱۳۱ قانون مجازات نیروهای مسلح ناظر بر مواد «۹۵، ۹۶، ۹۷، ۹۸، ۱۰۳، ۱۰۴ و ۱۰۶»^۱ قانون مزبور قرار گرفته و توأمأ عنصر قانونی بزه جعل رایانه‌ای را تشکیل می‌دهند. ماده ۱۳۱ قانون مجازات جرائم نیروهای مسلح برای اولین بار در ایران «داده‌های رایانه‌ای» را به عنوان موضوع جعل مطرح نموده و جعل رایانه‌ای را بزه‌انگاری کرد. بنابراین چنانچه یک نظامی به قصد تقلب اعمال مذکور در صدر ماده ۱۳۱ قانون مجازات جرائم نیروهای مسلح را مرتکب شود و محتوای داده‌های رایانه‌ای با مواد ۹۵ تا ۱۰۶ قانون مجازات جرائم نیروهای مسلح منطبق باشد، به جای جعل کلاسیک، جعل رایانه‌ای تحقق یافته و مرتکب حسب مورد مشمول مجازات یکی از مواد مذکور قرار خواهد گرفت.

^۱ - ماده ۹۵ قانون مجازات جرائم نیروهای مسلح: «هر نظامی که حکم یا امضاء یا مهر یا فرمان یا دستخط فرماندهی کل قوا را به اعتبار مقام وی جعل کند یا با علم به جعل و تزویر استعمال نماید به حبس از سه تا پانزده سال محکوم خواهد شد.»
ماده ۹۶ قانون مجازات جرائم نیروهای مسلح: «هر نظامی که حکم یا امضاء یا مهر یکی از فرماندهان و مسئولان نیروهای مسلح در رده فرمانده نیرو یا هم طراز و بالاتر را به اعتبار مقام آنان جعل کند یا با علم به جعل یا تزویر استعمال نماید به حبس از یک تا ده سال محکوم می‌شود.»

ماده ۹۷ قانون مجازات جرائم نیروهای مسلح: «هر نظامی که حکم یا امضاء یا مهر سایر فرماندهان و مسئولان نیروهای مسلح را به اعتبار مقام آنان جعل کند یا با علم به جعل یا تزویر استعمال نماید به حبس از یک تا پنج سال محکوم می‌شود.»
ماده ۹۸ قانون مجازات جرائم نیروهای مسلح: «هر نظامی که با مباشرت یا به واسطه، مهر یکی از نیروهای مسلح را جعل کند یا با علم به جعل و تزویر مورد استفاده قرار دهد به حبس از یک تا ده سال محکوم می‌شود.»

ماده ۱۰۳ قانون مجازات جرائم نیروهای مسلح: «هر نظامی که در احکام و تقریرات و نوشته‌ها و اسناد و سجلات و آمار و محاسبات و دفاتر و غیر آنها از نوشته‌ها و اوراق رسمی مربوط به امور نظامی و یا راجع به وظائفش جعل یا تزویر کند اعم از اینکه امضاء یا مهر یا خطوطی را تحریف کرده یا کلمه‌ای را الحاق کند یا اسامی اشخاص را تغییر دهد به حبس از دو تا پنج سال محکوم می‌گردد.»

ماده ۱۰۴ قانون مجازات جرائم نیروهای مسلح: «هر نظامی که در تحریر نوشته‌ها، قراردادها و مقاله‌نامه‌های راجع به وظایفش مرتکب جعل یا تزویر شود اعم از اینکه موضوع یا مضمون آن‌را تغییر دهد، گفته و نوشته یکی از مقامات یا تقریرات یکی از طرفها را تحریف کند یا امر باطلی را صحیح یا صحیحی را باطل یا چیزی را که به آن اقرار نشده اقرار شده جلوه دهد به حبس از دو تا پنج سال محکوم می‌شود.»

ماده ۱۰۶ قانون مجازات جرائم نیروهای مسلح: «هر نظامی که به مناسبت انجام وظیفه به یکی از طرق مذکور در اسناد و نوشته‌های غیر رسمی جعل و تزویر کند به حبس از شش ماه تا دو سال محکوم می‌شود.»



۲-۳-۲- رکن مادی

در بحث از عنصر مادی به ترتیب مطالبی را پیرامون رفتار مبزهانه، عمل و صور فعل مرتکب، موضوع بزه، خصوصیت مرتکب و تأثیر وسیله و نتیجه در وقوع بزه جعل در هر کدام از سه قانون مربوط به جعل رایانه‌ای در حقوق جزایی ایران (ماده ۶ قانون جرائم رایانه‌ای، ماده ۱۳۱ قانون مجازات جرائم نیروهای مسلح و ماده ۶۸ قانون تجارت الکترونیکی) و کنسوانسیون ساینبر بیان می‌نماییم به تعبیر دیگر عنصر مادی هر بزه‌ی مشکل می‌شود از عمل فیزیکی، شرایط و اوضاع و احوال و نتیجه به دست آمده که البته می‌باید بین عمل فیزیکی و نتیجه به دست آمده‌ی آن بزه رابطه علیت موجود باشد. در بحث عنصر مادی باید گفت که می‌توان استنباط نمود که جعل رایانه‌ای همانند جعل سنتی به دو گونه ارتکاب می‌یابد:

۱- جعل مادی ۲- جعل معنوی

جعل مادی عبارت از تغییر، وارد کردن، محو کردن و موقوف کردن داده‌هاست که دارای آثار خارجی محسوس و مشهود است، به گونه‌ای که با چشم یا با وسایل دقیق‌تر آثار خارجی آن قابل تشخیص باشد. جعل معنوی رایانه‌ای هم بدین ترتیب است که داده‌ها به صورت چاپ شده ارایه نشود، بلکه به طور مستقیم مثلاً در حین پردازش صورت گیرد. «این نکته در مورد بانک و معاملاتی که فرآیند آن تنها در کامپیوتر صورت می‌گیرد و نمود خارجی ندارد قابل مشاهده است»^۱ بیشترین مصادیق این نوع جعل در حقوق سنتی در ماده ۵۳۴ قانون مجازات اسلامی بیان شده است. اگر چه قانونگذار در مقرره‌های قانونی راجع به جعل رایانه‌ای در خصوص جعل معنوی هیچگونه اشاره‌ای ننموده است ولی با استنباط از مواد قانونی راجع به جعل سنتی می‌توان گفت که ارتکاب جعل معنوی رایانه‌ای به پنج روش امکان‌پذیر است: ۱- تغییر موضوع یا داده پیام ۲- تحریف داده پیام مربوط به یکی از مقامات رسمی ۳- تحریف داده پیام مرتبط به یکی از طرفین ۴- صحیح جلوه دادن امر باطل و یا باطل جلوه دادن امر صحیح ۵- اقرار جلوه دادن چیزی که بدان اقرار نشده است و یا بالعکس. از آنجا که رکن مادی در جعل مادی و جعل معنوی به صورت واحد می‌باشد و فی الواقع قانونگذار در جعل رایانه‌ای آنگونه که در جعل کلاسیک بیان شده است دست

۱ - خداقلی، زهرا، جرائم کامپیوتری، چاپ اول، انتشارات آریان، تهران، ۱۳۸۳، ص ۱۵۳.



به تفکیک این دو نوع جعل زده است و به صورت واحد آن را بیان کرده است ما هم به همین میزان که توضیح دادیم بسنده می‌کنیم و به صورت کلی عناصر متشکله رکن مادی جعل رایانه‌ای را بررسی می‌نماییم.

رفتار مرتکب

در این گفتار طی عناوین جداگانه رفتار مرتکب را در قوانین داخلی و همچنین کنوانسیون جرایم سایبر در مورد جعل رایانه‌ای بیان می‌داریم و طی عنوان دیگری شرایط رفتاری مزهانه‌ی جعل رایانه‌ای را بیان می‌داریم.

الف: رفتار مرتکب در ماده ۶ قانون جرائم رایانه‌ای

بزه جعل رایانه‌ای موضوع ماده ۶ قانون جرائم رایانه‌ای از فعل مثبت مرتکب تشکیل شده است و این بزه با ترک فعل تحقق پیدا نمی‌کند. رفتار مرتکب برای این بزه بر مبنای ماده ۶ قانون جرایم رایانه‌ای عبارتست از: تغییر، ایجاد و وارد کردن متقلبه‌ی داده و تغییر علائم موجود در کارتهای حافظه یا قابل پردازش در سامانه‌های رایانه‌ای یا مخابراتی یا تراشه‌ها: پس این افعال که حصری هستند عبارتند از: ۱- ایجاد کردن ۲- تغییر دادن ۳- وارد کردن که در مورد هر کدام از آنها توضیحاتی را ارائه می‌نماییم.

۱- ایجاد کردن داده‌ها

منظور از آن ایجاد یک داده‌ی جدید می‌باشد که هیچ‌یک از اجزاء آن از قبل وجود نداشته است. ایجاد یا ساختن یک داده جدید فقط از طریق وارد کردن داده‌ها امکان‌پذیر است. از طریق تغییر دادن یا حذف یا متوقف کردن داده‌ها نمی‌توان داده‌ای ایجاد کرد که از قبل هیچ‌یک از اجزاء آن وجود نداشته است. اگر یک کاربر رایانه‌ای که مشمول خدمت سربازی است، وارد سیستم‌های رایانه‌ای اداره نظام وظیفه شود و یک سند الکترونیکی ایجاد کند که منجر به معافیت او از خدمت سربازی شود عمل وی مصداق ایجاد یک داده غیر صحیح جدید از طریق وارد کردن عمدی و بدون حق داده‌هاست.

مثال دیگری که در خصوص ایجاد کردن داده می‌توان زد موردی است که با ورود به سیستم رایانه‌ای یک دانشگاه بزرگ و ایجاد یک پرونده تحصیلی که به صدور مدرک تحصیلی در آن دانشگاه برای فرد منجر شود، روبرو هستیم.