



کلیه حقوق مادی و معنوی مترتب بر نتایج، ابتکارات و نوآوری های ناشی از تحقیق موضوع این پایان نامه متعلق به « دانشگاه میبد» است و هرگونه استفاده از نتایج علمی و عملی این پایان نامه برای تولید دانش فنی، ثبت اختراع، ثبت اثر بدیع هنری، همچنین چاپ و تکثیر، نسخه بره داری، ترجمه و اقتباس و ارائه مقاله در سمینارها و مجلات علمی از این پایان نامه منوط به موافقت کتبی « دانشگاه میبد» است.



گروه فقه و حقوق اسلامی

پایان نامه

جهت دریافت درجه کارشناسی ارشد

فقه و حقوق جزا

عنوان:

بررسی فقهی، حقوقی هک

استاد راهنما:

دکتر سید احمد میر خلیلی

استاد مشاور:

دکتر عباس کلانتری خلیل آباد

تدوین کننده:

سید علی اکبر موسوی

نیمسال دوم ۹۶-۹۷

تقدیم

این پژوهش را تقدیم می‌کنم به آستان قدسی و ملکوتی حضرت فاطمه‌ی زهرا (سلام الله علیها)
و به ساحت نورانی صاحب العصر و الزمان حضرت بقیه الله الأعظم (أرواحنا له الفداء)

همچنین روح پاک پدر

، قلب ساده مادر

و دستان مهربان همسر

تشکر و قدردانی

بر خود لازم می دانم مراتب سپاس را از بزرگوارانی که اگر دست یاری گرمشان نبود، هرگز این پایان نامه به سرانجام نمی رسید:

از استاد مهربان و دلسوز، جناب آقای دکتر سید احمد میر خلیلی که زحمت راهنمایی این پایان نامه را بر عهده داشتند بسیار سپاس گذارم و همچنین از جناب آقای دکتر عباس کلانتری خلیل آباد که زحمت مشاوره این پایان نامه را متحمل شدند، صمیمانه تشکر می کنم.

چکیده

پیشرفت بشر در زمینه فضای مجازی اگرچه راه گشای بسیاری از مشکلات انسان در عصر معاصر بوده است؛ لکن ظرف و محلی برای ارتکاب برخی جرائم گشته است. هک از جمله جرائمی است که در فضای مجازی اتفاق می‌افتد، که می‌توان آن را به سه دسته تقسیم کرد. هک‌های کلاه‌سیاه، کلاه‌خاکستری و کلاه‌سفید؛ که می‌توان از هک‌های کلاه‌سیاه و کلاه‌خاکستری به‌عنوان دسترسی غیرمجاز به داده‌ها و خرابکاری داده‌ها در فضای مجازی نام برد. قانون‌گذار محترم در حمایت از داده‌ها، با اتکا به قواعد فقهی، مانند حرام بودن تجسس در امور دیگران، حرام بودن ضرر زدن به دیگران، حرام بودن وارد شدن به حریم خصوصی دیگران، حرام بودن تصرف بدون اجازه در اموال دیگران، مقدمه حرام و حرام بودن تخریب اموال دیگران در ماده ۱ و ۸ قانون جرائم رایانه‌ای به جرم‌انگاری دسترسی غیرمجاز داده‌ها و تخریب داده‌ها پرداخته است. در این تحقیق که با روش توصیفی-تحلیلی نگاشته شده، ثابت می‌گردد که هک‌های کلاه‌سیاه و کلاه‌خاکستری می‌تواند مصداقی برای دسترسی غیرمجاز و تخریب داده‌ها باشد، در ضمن دسترسی غیرمجاز و تخریب داده‌ها که در فضای مجازی واقع می‌شوند، ماهیت متفاوتی با دسترسی غیرمجاز و تخریب سنتی دارند. هک‌های کلاه‌سفید را می‌توان به‌وسیله قواعد فقهی همچون تسلط، امر به معروف و نهی از منکر و واجب بودن حفظ نظام و منع از اختلال نظام آن را قانونمند دانست. بر این اساس در بخش اول به کلیات و در بخش دوم به بررسی فقهی، حقوقی هک، هک‌های کلاه‌سیاه و کلاه‌خاکستری و در بخش سوم به بررسی فقهی هک، هک‌های کلاه‌سفید پرداخته شده است.

کلیدواژه‌ها: فضای مجازی، داده‌ها، هک، هک‌های کلاه‌سیاه، هک‌های کلاه‌خاکستری، هک‌های

کلاه‌سفید

فهرست مطالب

مقدمه.....	۱
۱. تبیین موضوع.....	۱
۲. ضرورت تحقیق.....	۲
۳. سابقه تحقیق.....	۲
۴. سوالات پژوهش.....	۳
۵. فرضیه های پژوهش.....	۴
۶. هدف تحقیق.....	۴
۷. روش تحقیق.....	۴
۸. ساختار تحقیق.....	۴

فصل اول: کلیات

۱-۱ مفاهیم.....	۶
۱-۱-۱ رایانه.....	۶
۱-۱-۲ شبکه.....	۶
۱-۱-۳ داده.....	۶
۱-۱-۴ اینترنت.....	۷
۱-۱-۵ فضای سایبری.....	۷
۱-۱-۵-۱ کارکردهای فضای سایبر.....	۸
۱-۱-۶ تعریف جرایم رایانه ای.....	۱۰
۱-۱-۷ تقسیم بندی جرایم رایانه ای.....	۱۱
۱-۱-۷-۱ جرایم علیه اشخاص.....	۱۱
۱-۱-۷-۲ جرایم علیه اموال و دارایی.....	۱۱
۱-۱-۷-۳ جرایم علیه دولت ها.....	۱۲
۱-۱-۸ ویژگی های جرایم رایانه ای.....	۱۲
۱-۱-۹ هک.....	۱۵
۱-۱-۹-۱ هک در لغت.....	۱۵
۱-۱-۹-۲ هک در اصطلاح.....	۱۵
۱-۱-۱۰ هکرها.....	۱۶
۱-۱-۱۰-۱ هکرهای کلاه سفید.....	۱۶
۱-۱-۱۰-۲ هکرهای کلاه سیاه.....	۱۷

- ۱-۱-۱-۱-۲-۱. گروه اسکرپیت کپی..... ۱۷
- ۱-۱-۱-۲-۲-۱. گروه وب..... ۱۷
- ۱-۱-۱-۳-۲-۱. گروه هکرهای آتشنزن..... ۱۸
- ۱-۱-۱-۴-۲-۱. گروه هکرهای سیاه قانونی..... ۱۸
- ۱-۱-۱-۳-۱-۱. هکرهای کلاه خاکستری..... ۱۸
- ۱-۱-۱-۴-۱-۱. روشهای هک کردن..... ۱۹
- ۱-۲-۱. تاریخچه هک..... ۲۰

فصل دوم: مبانی فقهی، حقوقی حکم هک هکرهای کلاه سیاه و کلاه خاکستری

- ۱-۲-۱. دسترسی غیرمجاز..... ۲۴
- ۱-۱-۲-۱. حرمت تجسس در امور دیگران..... ۲۷
- ۱-۱-۱-۲-۱. مبانی حرمت تجسس..... ۲۸
- ۱-۱-۲-۲-۱. تطبیق قاعده مزبور در بزه «دسترسی غیرمجاز به داده‌ها»..... ۲۹
- ۱-۱-۲-۲-۲. حرام بودن ضرر زدن به دیگران..... ۲۹
- ۱-۲-۱-۲-۱. مبانی حرمت ضرر زدن دیگران..... ۳۰
- ۱-۲-۲-۲-۱. تطبیق قاعده مزبور بر بزه «دسترسی غیرمجاز به داده‌ها»..... ۳۱
- ۱-۲-۳-۱. حرمت وارد شدن بدون اذن به حریم خصوصی دیگران..... ۳۲
- ۱-۳-۱-۲-۱. مبانی فقهی حریم خصوصی..... ۳۳
- ۱-۳-۲-۲-۱. تطبیق قاعده مزبور بر بزه «دسترسی غیرمجاز به داده‌ها»..... ۳۴
- ۱-۳-۴-۱. حرام بودن اذیت رساندن به دیگران..... ۳۴
- ۱-۴-۱-۲-۱. مبانی فقهی آزار و اذیت دیگران..... ۳۵
- ۱-۴-۲-۲-۱. تطبیق قاعده مزبور بر بزه «دسترسی غیرمجاز به داده‌ها»..... ۳۵
- ۱-۵-۱-۲-۵. حرام بودن تصرف بدون اجازه در اموال دیگران..... ۳۶
- ۱-۵-۱-۲-۱. مبانی فقهی حرام بودن تصرف بدون اجازه در اموال دیگران..... ۳۶
- ۱-۵-۲-۲-۱. تطبیق قاعده مزبور بر بزه «دسترسی غیرمجاز به داده‌ها»..... ۳۷
- ۱-۶-۱-۲-۶. مقدمه حرام..... ۳۷
- ۱-۷-۱-۲-۷. ارکان تشکیل‌دهنده..... ۳۸
- ۱-۷-۱-۲-۱. رکن قانونی جرم دسترسی غیرمجاز..... ۳۸
- ۱-۷-۲-۲-۱. رکن مادی جرم دسترسی غیرمجاز..... ۴۱
- ۱-۷-۳-۲-۱. رکن روانی جرم دسترسی غیرمجاز..... ۴۸
- ۱-۲-۲-۲. تخریب در داده‌ها..... ۵۰
- ۱-۲-۲-۱. ویژگی‌های جرم تخریب..... ۵۱
- ۱-۲-۲-۲. حرام بودن تخریب اموال دیگران..... ۵۲

- ۵۲..... ۱-۲-۲-۲. مبانی حرام بودن تخریب اموال دیگران.
- ۵۳..... ۲-۲-۲-۲. تطبیق قاعده مزبور بر بزه «تخریب داده‌ها».
- ۵۳..... ۴-۲-۲. حرام بودن تصرف غیر مجاز در اموال دیگران.
- ۵۴..... ۱-۴-۲-۲. تطبیق قاعده مزبور بر بزه «تخریب داده‌ها».
- ۵۴..... ۵-۲-۲. حرام بودن اذیت دیگران.
- ۵۴..... ۶-۲-۲. ارکان تشکیل‌دهنده.
- ۵۴..... ۱-۶-۲-۲. عنصر قانونی.
- ۵۶..... ۲-۶-۲-۲. عنصر مادی.
- ۶۲..... ۳-۶-۲-۲. عنصر روانی.

فصل سوم: مبانی فقهی حکم حکم هکرهای کلاه‌سفید

- ۶۵..... ۱-۳. قاعده تسلط.
- ۶۶..... ۱-۱-۳. مبانی فقهی قاعده تسلط.
- ۶۶..... ۲-۱-۳. تحلیل قاعده تسلط.
- ۶۷..... ۳-۱-۳. تطبیق قاعده تسلط بر هکرهای کلاه‌سفید.
- ۶۷..... ۲-۳. امر به معروف و نهی از منکر.
- ۶۸..... ۱-۲-۳. مبانی فقهی امر به معروف و نهی از منکر.
- ۶۹..... ۲-۲-۳. منکر در فضای مجازی.
- ۷۰..... ۱-۲-۲-۳. جرائم علیه تمامیت جسمانی.
- ۷۰..... ۲-۲-۲-۳. جرائم علیه اخلاق و عفت عمومی.
- ۷۰..... ۱-۲-۲-۲-۳. پورنوگرافی.
- ۷۱..... ۲-۲-۲-۲-۳. تورسیم سکسی.
- ۷۲..... ۳-۲-۲-۲-۳. تبلیغ قوادی.
- ۷۲..... ۴-۲-۲-۲-۳. تبلیغ و ایجاد سایت برای ارتباطات نامشروع.
- ۷۳..... ۵-۲-۲-۲-۳. ایجاد و تبلیغ سایت برای قمار.
- ۷۳..... ۳-۲-۳. تطبیق قاعده امر به معروف و نهی از منکر بر هکرهای کلاه سفید.
- ۷۵..... ۳-۳. واجب بودن حفظ نظام و منع از اختلال نظام.
- ۷۵..... ۱-۳-۳. مبانی فقهی قاعده واجب بودن حفظ نظام.
- ۷۴..... ۱-۱-۳-۳. آیات دال بر نهی از فساد.
- ۷۶..... ۲-۱-۳-۳. تعیین مجازات برای اخلاک‌گران در نظام.
- ۷۶..... ۳-۱-۳-۳. دلالت روایات بر وجوب حفظ نظام و منع از اختلال نظام.
- ۷۸..... ۴-۱-۳-۳. بنای عقلا بر وجوب حفظ نظام و منع از اختلال.
- ۷۸..... ۲-۳-۳. مصادیق اختلال نظام در فضای مجازی.

- ۳-۲-۱. جنجال‌سازی و فضای‌سازی رسانه‌ای از طریق وبلاگ‌ها..... ۷۹
- ۳-۲-۲. ایجاد و گسترش تنش‌های اجتماعی متراکم و گسترده از طریق شبکه‌های اجتماعی..... ۷۹
- ۳-۲-۳. سلب اعتماد اجتماعی..... ۸۱
- ۳-۲-۴. توانمندسازی جنبش‌های مدنی و سیاسی بر علیه نظام..... ۸۱
- ۳-۲-۵. انجام عملیات تروریسم سایبری بر علیه نظام..... ۸۲
- ۳-۲-۱. مفهوم و ماهیت تروریسم..... ۸۲
- ۳-۲-۲. عناصر مشترک تروریسم..... ۸۳
- ۳-۲-۳. فضای سایبری در خدمت تروریسم..... ۸۴
- ۳-۲-۶. تطبیق قاعده واجب بودن حفظ نظام و حرام بودن اختلال نظام بر هکرهای کلاه‌سفید..... ۸۵
- نتیجه‌گیری..... ۸۶
- پیشنهادها..... ۸۷
- منابع و مأخذ..... ۸۸

مقدمه

یکی از اقسام مسئولیت‌های کیفری پیش‌بینی‌شده توسط مقنن، جرائم و مجازاتی است که برای جرائم رایانه‌ای وضع شده است. ماده ۱(۷۲۹ ق.م.ا) از این قانون به دسترسی غیرمجاز داده‌ها می‌پردازد و ماده ۸(۷۳۶ ق.م.ا) این قانون بیان‌گر مجازات تخریب و اخلال در داده‌ها هست.

در این پژوهش بر آنیم تا ضمن تطبیق این مواد بر مسئله هک و ارائه مبانی فقهی این مسئولیت به بررسی ارکان تشکیل‌دهنده مسئولیت کیفری مزبور پرداخته شود.

۱- تبیین موضوع

انسان مدرن در اواخر قرن نوزدهم و اوایل قرن بیستم وارد دوران صنعتی و فرا صنعتی شد که آن را فضای سایبری می‌نامند و با پیدایش دنیای سایبری در جهان امروز پیامدهای مثبت و منفی برای جهان بشری اتفاق افتاد، از جمله پیامدهای منفی آن پیدایش جرائمی با عنوان جرائم رایانه‌ای شده است. این جرائم برخلاف ظاهر آرام و بی‌خطر بودنشان بسیار خطرناک می‌باشند؛ به گونه‌ای که سبب به وجود آمدن جرائم بسیاری از جمله قتل، خودکشی، سرقت، کلاهبرداری و... شده‌اند.

می‌توان بیان داشت، عمده‌ترین عنوان مجرمانه‌ای که در حوزه فضای مجازی اتفاق می‌افتد، مسئله هک است. اولین اقدام برای شروع اکثر جرائمی که در فضای مجازی واقع می‌شوند دسترسی غیرمجاز به داده و اطلاعات هر سیستم رایانه‌ای است. این ورود غیرمجاز، می‌تواند به انگیزه خرابکاری، صدمه زدن به داده‌ها، اطلاعات، صدمه زدن به سیستم شخص مقابل، دزدی اطلاعات و کنجکاوی باشد.

با توجه به اصل قانونی بودن جرم و مجازات در قانون ایران، قانون‌گذار در سال ۱۳۸۸/۳/۵ قانون جرائم رایانه‌ای را تصویب کرد و مجازات دسترسی غیرمجاز به داده‌ها در ماده ۱، و تخریب داده‌ها در ماده ۸ قانون جرائم رایانه‌ای بیان شده است. به نظر می‌رسد اشکالاتی به این مواد از قانون وارد است؛ از جمله بیان نکردن مستثنیات این جرائم یعنی زمانی که این دسترسی غیرمجاز به داده‌ها و تخریب و اخلال در داده‌ها برای امر مهمی از قبیل حفظ نظام، امر به معروف و نهی از منکر و... باشد.

از آن‌رو که قانون مجازات اسلامی ایران برگرفته از قواعد فقهی است و با توجه به این‌که دین مقدس اسلام دین کاملی می‌باشد و برای همه موضوعات حکمی دارد و هیچ موضوعی را بدون حکم نگذاشته است، یکی از موضوعات فقهی بررسی حکم هک است، که بایستی مبانی فقهی و حقوقی حکم آن مورد بررسی قرار گیرد و این پایان‌نامه در مقام بیان آن است.

از جمله اهدافی که در این پژوهش به آن‌ها می‌پردازیم آگاهی مردم، بالأخص جوانان نسبت به حکم فقهی هک در فضای مجازی است و از طرفی روشن شدن حکم موضوع برای قانون‌گذار است تا نسبت به اصلاح و تکمیل قوانین موجود اقدام نماید.

۲. ضرورت تحقیق

با توجه به این مسئله که دین اسلام کاملترین دین الهی، باید جوابگو مسائل محدث باشد. یکی از این مسائل در رابطه به هک می باشد لذا ضرورت دارد که با استفاده از قواعد فقهی و حقوقی اسلامی حکم این مسئله بیان شود.

۳. سابقه تحقیق

هک از جمله مسائل جدیدی است که سابقه‌ی چندانی در فقه و حقوق ندارد. پژوهشگرانی که در رابطه با هک تحقیقاتی را انجام داده‌اند، به تعریف از هک، ماهیت آن، انواع آن، جنبه حقوقی و یا به مسائل اخلاقی مرتبط به فضای مجازی پرداخته‌اند. ولی به نظر می‌رسد در این تحقیقات صورت گرفته به‌طور شایسته به جنبه‌های فقهی و حقوقی هک پرداخته نشده است. در این پژوهش بر آن شدیم تا مبانی فقهی، حقوقی هک را مورد بررسی قرار دهیم. از بین کتاب‌ها، پایان‌نامه‌ها و مقاله‌ها می‌توانیم به این آثار اشاره کرد.

الف. کتاب‌ها

راهنمای گام‌به‌گام نفوذ به کامپیوترها و راههای مقابله با آن به نویسندگی اسکو دیس اد، (مترجمین، ابوالفضل طاهری ریزی و آرزو خسروپور) انتشارات توانا. (۱۳۸۳ ه ش) نویسنده در این کتاب فقط به تعریف و ماهیت هک پرداخته است اما بحث فقهی، حقوقی هک را بیان نکرده است.

آشکارسازی هک به نویسندگی دیویس، مایکل آ (مترجم، علی نایب پور) (۱۳۸۴ ه ش) انتشارات نگارستان اندیشه. نویسنده در این کتاب فقط به تعریف و ماهیت هک پرداخته است اما بحث فقهی، حقوقی هک را بیان نکرده است.

اصول و مفاهیم هک و نفوذ به نویسندگی محمدجواد کریمی (۱۳۹۳ ه ش) نویسنده در این کتاب فقط به ماهیت و تعریف هک پرداخته است اما بحث فقهی، حقوقی هک را بیان نکرده است.

امنیت شبکه‌ها کامپیوتر و اصول هک به نویسندگی هومن همایون (۱۳۸۲ ه ش) نویسنده در این کتاب فقط به اصول هک پرداخته است اما بحث فقهی، حقوقی هک را بیان نکرده است.

ب. پایان‌نامه‌ها

بررسی صلاحیت جزائی در جرائم سایبری به نویسندگی محسن اجنگان فاردقی (۱۳۹۱ ه ش) دانشگاه تبریز، دانشکده حقوق سیاسی، نویسنده در این پایان‌نامه، به بحث حقوقی جرائم سایبری و حکم پرداخته است اما بحث فقهی حکم را بیان نکرده است.

سیاست جنایی قضایی ایران در قبال جرائم رایانه‌ای به نویسندگی سعید سلطانی (۱۳۹۳ ه ش) دانشگاه تربیت مدرس، دانشکده ادبیات و علوم انسانی، نویسنده در این پایان‌نامه، به بحث حقوقی جرائم رایانه‌ای پرداخته است اما بحث فقهی جرائم رایانه‌ای را بیان نکرده است.

خرابکاری رایانه‌ای در قانون جرائم رایانه‌ای ایران به نویسندگی مریم عطوان (۱۳۹۱ ه ش) دانشگاه اصفهان، دانشکده حقوق و علوم سیاسی، نویسنده در این پایان‌نامه به بحث حقوقی جرائم رایانه‌ای پرداخته است اما بحث فقهی آن را بیان نکرده است.

ج. مقاله‌ها

بررسی پدیده جرائم اینترنتی در ایران و جهان به نویسندگی زهره سکنی، چاپ‌شده در مجله اصلاح و تربیت شماره ۲۴ (۱۳۸۲ ه ش) نویسنده در این مقاله، فقط به بررسی جرائم اینترنتی و فضای سایبری پرداخته است اما بحث فقهی در رابطه با حکم را بیان نکرده است.

هکرها در دام قانون به نویسندگی هستی طهماسبی، چاپ‌شده در مجله گزارش شماره ۱۵۵ (۱۳۸۳ ه ش) نویسنده در این مقاله به بررسی حکم حکم در قانون پرداخته است اما بحث فقهی در رابطه با حکم را بیان نکرده است.

جرم و کامپیوتر به نویسندگی محسن طاهری، چاپ‌شده در مجله حقوقی دادگستری شماره ۳۴۹ (۱۳۷ ه ش) نویسنده در این مقاله، به بررسی حکم حکم در قانون پرداخته است اما بحث فقهی در رابطه با حکم را بیان نکرده است.

۴. سؤالات پژوهش

۱- سؤال اصلی

مبانی فقهی، حقوقی حکم حکم چیست؟

۲-سؤالات فرعی

الف مبانی فقهی حکم هک، هکرهای کلاه‌سیاه و کلاه خاکستری و مسئولیت کیفری آن چیست؟

ب مبانی فقهی هک، هکرهای کلاه‌سفید چیست؟

۵. فرضیه های پژوهش

الف. فرضیه اصلی

در قانون مجازات اسلامی ایران، تحت ماده‌های مختلفی مجازات هک بیان شده است و به دلیل اینکه قانون مجازات ایران برگرفته از فقه می‌باشد طبق قواعد مثل لا ضرر، حرمت غصب و... می‌توانیم حکم به حرمت را در مسئله هک جاری کرد.

ب. فرضیات فرعی

۱. مسئله هک چون از جمله مسائل نوظهور است و سابقه‌ای طولانی در فقه ندارد. باین حال بر اساس مبانی که در فقه وجود دارد (قاعده لا ضرر، حرمت غصب و...) می‌توان گفت حکم هک، در هکرهای کلاه‌سیاه و کلاه خاکستری حرمت است.

۲. با توجه به قواعدی مانند امر به معروف و نهی از منکر، حفظ نظام و... که در رابطه با هک کردن هکرهای کلاه‌سفید جاری می‌شود می‌توان حکم به مباح بودن هک، هکرهای کلاه‌سفید داد.

۶. هدف تحقیق

هدف از تحقیق پیش رو، تبیین حکم فقهی، حقوقی هک و تطبیق آن به دسترسی غیر مجاز به داده ها و تخریب و اخلاف در داده ها می باشد.

۷. روش تحقیق

این پایان‌نامه، به روش تحلیلی و توصیفی انجام خواهد شد و جمع‌آوری اطلاعات به شیوه کتابخانه‌ای می‌باشد؛ ضمن آنکه از تمامی ابزارها و لوازم رایانه‌ای و پایگاه اطلاع‌رسانی استفاده خواهد شد.

۸. ساختار تحقیق

فصل اول به کلیات بحث اختصاص دارد که مطالب بعدی با اتکا بر آن‌ها شکل خواهد گرفت. در فصل دوم به بررسی فقهی و حقوقی هکرهای کلاه‌سیاه و کلاه خاکستری می‌پردازیم، و در فصل سوم به بررسی فقهی هکرهای کلاه‌سفید پرداخته خواهد شد.

۱ فصل اول: کلیات

۱-۱ مفاهیم

برای بررسی فقهی، حقوقی هک و همچنین بیان مقصود نگارنده، تحلیل و بررسی واژگان مرتبط با پژوهش پیش رو امری ضروری است.

۱-۱-۱ رایانه

در تعریف رایانه^۱ گفته شده است: «رایانه، سیستمی است که می‌توان داده‌ها، اطلاعات و برنامه‌های گوناگونی را در حافظه‌اش نگهداری کند و مطابق با دستوراتی که به او داده می‌شود و یا همان برنامه‌هایی که برای او برنامه‌ریزی شده است، اطلاعات را واکاوی کند و پس از واکاوی به صورت گزارش یا اطلاعات ارائه کند.»^۲

به عبارت ساده‌تر می‌توان گفت: رایانه می‌تواند از مجموعه عظیمی از دستورها به نام برنامه پیروی کند، این امر به آن اجازه می‌دهد تا قابلیت انجام طیف وسیعی از وظایف را داشته باشد؛ و بر اساس برنامه‌ای که به آن داده می‌شود عمل می‌کند.

۱-۱-۲ شبکه

در تعریف «شبکه»^۳ گفت شده است: شبکه، متشکل از چند کامپیوتر مرتبط با یکدیگر است،^۴ و با در ارتباط بودن باهم یک شبکه را تشکیل داده‌اند.

در طول سالیان گذشته میلیون‌ها کامپیوتر به شکل شبکه به یکدیگر متصل شده‌اند. این شبکه امکان تبادل داده میان کامپیوترهای مختلف و به اشتراک‌گذاری منابع را فراهم کرده است.

۱-۱-۳ داده

در تعریف داده^۵ گفته شده است: «داده یک جزء اطلاعاتی است.»^۶ داده می‌تواند شامل همه آگاهی‌ها، شناسه‌ها، آمارها دانسته‌ها، داشته‌ها، پنداشته‌ها و ... باشد. باید توجه داشت که دو کلمه داده و اطلاعات^۷

۱. computer

۲. آریا، ناصر، فرهنگ اصطلاحات کامپیوتر و شبکه‌های کامپیوتر، ناشر دانشگاه شریف، تهران، ۱۳۷۲ ه.ش، ص ۳۲

۳. Network

۴. همان، ص ۱۱۴

۵. data

۶. قلی زاده نوری، فرهاد، فرهنگ تشریحی اصطلاحات کامپیوتری، انتشارات آذر، تهران، ۱۳۸۳ ه.ش، ص ۲۳

۷. Information

در دنیای کامپیوتر بسیار استفاده می‌شوند این دو لغت دارای معنی متفاوت هستند.^۱ برای درک موضوع به مثال زیر توجه فرمایید:

به‌عنوان مثال عدد ۲۰۲۰ یک داده است وقتی که کامپیوتر این داده را به‌عنوان تاریخ تفسیر می‌کند این داده معنی پیدا می‌کند و از آن لحظه به بعد به آن اطلاعات گفته می‌شود بنابراین می‌توان نتیجه گرفت که اطلاعات از داده‌ها به وجود می‌آیند.

۱-۱-۴ اینترنت

در تعریف اینترنت بیان شده است: «اینترنت کوتاه شده International newtorking می‌باشد و شبکه‌ای از شبکه‌هاست.»^۲

وزارت دفاع آمریکا در سال ۱۹۶۹ میلادی که در زمینه مسائل دفاعی تحقیق می‌کرد، شبکه‌ای را طراحی کرد تا کامپیوترهای بسیاری باهم در ارتباط باشند. نام این شبکه را آرپانت^۳ گذاشتند. کم‌کم کامپیوترهای دانشگاه‌های مختلف هدف شبکه آرپانت قرار گرفت و برای اطلاعات در زمینه‌های مختلف تحقیقاتی در رشته‌های بزرگ در ایالات متحده آمریکا مورد استفاده قرار گرفت، به تدریج کشورهای مختلف دنیا به این شبکه پیوستند که در سال ۱۹۷۷ میلادی نام آرپانت به اینترنت تغییر یافت و سپس در سال ۱۹۹۰ میلادی اینترنت جهانی شد.^۴ در حال حاضر میلیون‌ها کامپیوتر در سراسر جهان به این شبکه پیوسته‌اند و شبکه جهانی اینترنت را به وجود آوردند؛ و هر شخص، در هر جای از کره زمین قرار دارد می‌تواند به این شبکه عظیم جهانی متصل شود.

۱-۱-۵ فضای سایبری

سایبر^۵ واژه‌ای انگلیسی است که از ریشه یونانی گرفته شده است. «در زبان یونانی به معنای راندن و حکومت کردن به کاررفته است امروزه به معنای حضور در فضای اینترنت است.»^۶ این امر نشان می‌دهد که این واژه تا چه اندازه از معنای اصلی خود دور شده است.

۱. خلیق، غلامرضا، رایانه ای کار درجه ICDL۲ تحت ویندوز ۷ نگارش ۵، انتشارات راهی، تهران، ۱۳۹۰ ه ش،

ص ۱۷

۲. شلی اوهارا، آموزش سریع مبانی کامپیوتر و داده پردازی، مترجم؛ عاصی، هادی، انتشارات راوی مهر،

تهران، ۱۳۸۲ ه ش، ص ۱۰۹

۳. ARPANET

۴. گروه مؤلفین بتیاد ICDL، آموزش اینترنت بتیاد ICDL، گنج، تهران، ۱۳۹۰ ه ش، ص ۱

۵. Cyber

۶. اثنی عشران، مهدی، وقف سایبری، مجله جاویدان، ۱۳۹۰ ه ش، شماره ۷۵، ص ۷

در زبان فارسی لغت سایبر به مجاز و مجازی اطلاق شده است.^۱ می‌توان گفت، این معنا بیانگر دقیق این واژه نمی‌تواند قرار بگیرد، مجاز در مقابل حقیقت به کار می‌رود، به معنای دیگر محیط سایبری، محیطی واقعی است. در واقع جهان سایبری هرچند به شکل ملموس و مادی قابل حس و لمس کردن نیست؛ اما همان‌گونه که به اطلاعات به وجود آمده از شیء نمی‌توان عنوان مجازی داد و در رابطه‌ی آنها نمی‌توان گفت حقیقت واقعی ندارند به همین دلیل به جهان سایبری نیز نمی‌توان اطلاق مجاز و مجازی کرد. با توجه به این مطلب که در زبان فارسی واژه‌ای، مترادف و هم‌معنای این عبارت باشد، یافت نمی‌شود استفاده از عبارت فضای مجازی^۲ و جرم‌های جهان مجازی^۳ رو به گسترش است، که در آینده جانشین عباراتی همانند جرم‌های رایانه‌ای و جرم‌های اینترنتی می‌شوند. برای فضای سایبری ویژگی‌هایی بیان شده که می‌توان آنها را به این صورت بیان کرد:

الف: دستیابی به اطلاعات

عدم محدودیت اشخاص در دستیابی به هرگونه اطلاعات و خدمات^۴، بدون اینکه این اطلاعات و خدمات در کدام نقطه از جهان به وجود آمدند و به کاربران ارائه شده‌اند.

ب: ارتباط کاربران با یکدیگر

ارتباط کاربران با یکدیگر و استفاده از اطلاعات آنها^۵، این امر در فضای سایبری به راحتی صورت می‌گیرد.

ج: انجام معاملات

انجام معاملات تجاری در فضای سایبری به راحتی انجام می‌گیرد و در این فضا انجام معاملات در سطح بین‌المللی^۶، روزبه‌روز در حال رشد می‌باشد.

با توجه به ویژگی‌های مذکور و امنیت ناکافی و طبیعت مجازی آن، فرصت بسیار مناسبی در اختیار افراد شرور قرار گرفته تا جرائمی همچون تخریب داده‌ها، اخلاص در داده‌ها، جعل و... را مرتکب شوند.

۱. زندی، محمدرضا، تحقیقات مقدماتی در جرایم سایبری، انتشارات جنگل جاودانه، تهران، ۱۳۹۳ ه. ش، ص ۲۱

۲. cyber space

۳. cyber crime

۴. محسنی دهکلانی، محمد، بررسی فقهی و حقوقی جرایم در عالم مجازی، کارشناسی ارشد حقوق جزاء، دانشگاه

مازندران، ۱۳۹۱ ه. ش، ص ۷۶

۵. همان

۶. اله وردی، فرهاد، همان کتاب، ص ۹

۱-۵-۱-۱ کارکردهای فضای سایبری (مجازی)

برای فضای مجازی کارکردها و قابلیت‌های مهمی وجود دارد که می‌توان آن‌ها را به این صورت برشمرد:

۱- پست الکترونیکی

بعد از وارد شدن کاربر به سیستم، پیغام و آدرس فرد موردنظر خود را ثبت نموده و سپس پیغام مزبور از مسیر پرپیچ‌وخم کامپیوترهای اتصال داده متعدد می‌گذرد و به مقصد موردنظر می‌رسد.^۱ می‌توان بیان داشت که ایمیل از قدیمی‌ترین خدمات به شمار می‌رود.

۲- گروه‌های خبری

گروه‌های خبری به خدماتی گفته می‌شود که شبیه پست الکترونیکی است، با این تفاوت که به جای ارسال پیغام به یک شخص، کاربر آن را به محل اشتراکی پست می‌کند،^۲ و بسیاری از کاربران دیگر می‌توانند آن‌ها را مشاهده کنند و به آن‌ها جواب دهند.

می‌توان بیان کرد گروه‌های خبری منبع اطلاعاتی مناسبی هستند برای اشخاص به‌عنوان مثال، برای خواندن مقاله‌های گروه‌های خبری، یا ارسال پیغام، دیدن فیلم و عکس و... می‌توان در آن‌ها عضو شد. با قرار دادن این موارد در آن گروه خبری کاربران زیادی به آن‌ها دست پیدا می‌کنند.

۳- چت

چت سیستمی است که کاربران از طریق آن می‌توانند در مورد مسئله خاص به گفت و گو و مکالمه بنشینند.^۳ این مکالمه از طریق تایپ انجام و سؤال‌ها و یا پاسخ افراد که در گفت‌وگو قرار دارند نیز بر روی صفحه‌نمایش رایانه قابل مشاهده است.

۵- یوتیوب

یوتیوب که در سال ۲۰۰۵ ایجاد شد. کاربران در این وبگاه در مرحله اول ثبت‌نام کرده و می‌توانند مقدار نامحدودی فیلم را در این وبگاه بارگذاری کنند و دیگر کاربران به راحتی می‌توانند به آن‌ها

^۱ . میر محمدی، داود، فضای مجازی و تحولات هویتی، انتشارات تمدن ایرانی، تهران، ۱۳۹۱ ه ش، ص ۴۰

^۲ همان

^۳ .امیدی، مریم، بررسی میزان و نوع استفاده از اینترنت و نقش آن در یادگیری مهارت‌های ارتباطی دانشجویان کارشناسی دانشکده روانشناسی و علوم تربیتی دانشگاه علامه طباطبایی، کارشناسی ارشد روانشناسی عمومی و میان رشته ای، دانشگاه علامه طباطبایی تهران، ۱۳۹۰ ه ش، ص ۵۴

دسترسی پیدا کنند. مسئولین یوتیوب اعلام کردند که کاربرانش روزانه صدها میلیون فیلم با موضوعات مختلف را در این وبگاه بارگذاری و یا تماشا می‌کنند.^۱

۱-۱-۶ تعریف جرائم رایانه‌ای

در تعریف جرم رایانه‌ای بیان شده است: «که هر فعل یا ترک فعلی که علیه شبکه‌ها یا رایانه صورت می‌گیرد، جرم رایانه‌ای است.»^۲

با گسترش وسیع در استفاده از اینترنت، شبکه‌های اجتماعی و ابزارهایی که متعلق به فضای سایبری هستند از قبیل: دستگاه‌های پرداخت، تلفن همراه، رایانه و... در زندگی فردی اشخاص و کارهای اداری، تخلف و بزهکاری در استفاده از این ابزارها نیز، اجتناب‌ناپذیر است. آنچه امروز تحت عنوان جرائم اینترنتی، جرائم رایانه‌ای و جرائم فضای سایبری نام‌برده می‌شود، مجموعه‌ای از همین بزهکاری‌ها و تخلفات است که از طریق اینترنت، رایانه و ابزارهای متعلق به این فضا واقع می‌شود.

۱-۱-۷ تقسیم‌بندی جرائم رایانه

جرائم رایانه‌ای را می‌توان به این صورت بیان کرد:

۱-۱-۷-۱ جرائم علیه اشخاص

رایانه وسیله‌ای برای انجام انواع جرائم علیه اشخاص می‌باشد. از قبیل:

الف- تصاویر و مطالب غیر مجاز

به تصویر کشیدن یا فروش عکس‌ها، نوشته‌هایی و فیلم‌های مبتذل^۳ جهت تحریک نوجوانان و جوانان و یا پیدا کردن اشخاص به‌وسیله‌های مختلف و معرفی آن‌ها به اشخاص دیگر در جهت ارتباط نامشروع.

ب- آزار و اذیت دیگران

این جرم می‌تواند به‌صورت مسخره کردن، متلک گفتن، بی‌حرمتی به ادیان و مقدسات دیگران و ... باشد.

۱. همان

۲. بای، حسینعلی، و پور قهرمانی، بابک، بررسی فقهی و حقوقی جرایم رایانه‌ای، انتشارات پژوهشگاه علوم و

فرهنگ اسلامی، قم، ۱۳۸۸ ه ش، ص ۳۹

۳. ابوبکری، محمد رؤف، بررسی جرم شناختی جرایم رایانه‌ای با توجه به قانون جرایم رایانه‌ای، دانشگاه تهران،

۱۳۹۳ ه ش، ص ۴۷