

دانشگاه پیام نور

مرکز مشهد

پایان نامه برای دریافت درجه کارشناسی ارشد در

رشته الهیات

گرایش: فقه و مبانی حقوق اسلامی

عنوان پایان نامه: بررسی فقهی حقوقی هکرهای سایبری در حوزه پول و
معاملات اقتصادی

استاد راهنما:

دکتر زهرا گواهی

استاد مشاور:

دکتر مهدی کریمی

نگارنده:

سمانه خالقی

مرداد 1396

ب



تاریخ: ۱۳۹۶/۱۱/۱۵

شماره:

پیوست: ۱۳۲۱/۲۵۶۱۹

صور تجلسه دفاع از پایان نامه کارشناسی ارشد

آقای/خانم سمانه خالقی

دانشجوی رشته الهیات گرایش فقه و مبانی حقوق اسلامی

به شماره دانشجویی ۹۴۹۵۲۳۲۹۱

تحت عنوان:

بررسی فقهی حقوقی هکرهای سایبری در حوزه پول و معاملات اقتصادی

جلسه دفاع پایان نامه کارشناسی ارشد نامبرده با حضور هیأت داوران در تاریخ: ۱۳۹۶/۰۶/۲۷ ساعت ۱۰ در محل مرکز مشهد برگزار و پس از ارزیابی پایان نامه مذکور به شرح زیر ارزیابی گردید.

نمره نهایی	دستاوردهای پژوهشی *	دفاع بر مبنای ۱۸	
۱۸/۵	۱/۵	۱۸	به عدد
۱۸/۵	۱/۵	۱۸	به حروف
	درجه ارزشیابی		

امضاء	محل خدمت	مرتبه دانشگاهی	نام و نام خانوادگی	هیأت داوران
	دانشگاه پیام نور مرکز مشهد	استادیار	دکتر زهرا گواهی	استاد راهنما
	دانشگاه پیام نور مرکز مشهد	استادیار	دکتر مهدی کریمی	استاد مشاور
	دانشگاه پیام نور مرکز مشهد	استادیار	دکتر محسن لعل علیزاده	استاد داور
	دانشگاه پیام نور مرکز مشهد	استادیار	دکتر اعظم امینی	نماینده تحصیلات تکمیلی

نمره نامبرده بر اساس بخشنامه‌ها و دستورالعمل‌های مربوط به دستاوردهای پژوهشی مستخرج محاسبه و در تاریخ ۱۳۹۶/۱۱/۱۵ نهایی شده است.

نام و امضای کارشناس پژوهشی مرکز مشهد

* نمره دستاورد پژوهشی برابر دستورالعمل مربوط در مهلت مقرر پس از دفاع تعیین شده و توسط کارشناس پژوهشی محاسبه و نمره نهایی اعلام می گردد.

مشهد: بولوار معلم - معلم - ۷۱ - صندوق پستی ۴۳۳ - ۹۱۷۳۵

نشانی الکترونیکی: info@pnum.ac.ir

تلفن: ۰۵۱۱ - ۸۶۸۳۹۰۰ (خط ۲۰) نمابر: ۰۵۱۱ - ۸۶۸۳۰۰۱ نمابر دبیرخانه: داخلی ۵۷۹

(گواهی اصالت نشر و حقوق مادی و معنوی اثر)

این جانب سمانه خالقی دانشجوی ورودی سال 1394 مقطع کارشناسی ارشد رشته الهیات گرایش فقه و مبانی حقوق اسلامی گواهی می‌نمایم چنانچه در پایان‌نامه خود از فکر، ایده و نوشته دیگری بهره گرفته‌ام با نقل قول مستقیم یا غیر مستقیم منبع و مأخذ آن را نیز در جای مناسب ذکر کرده‌ام. بدیهی است مسئولیت تمامی مطالبی که نقل قول دیگران نباشد بر عهده خویش می‌دانم و جوابگوی آن خواهم بود. دانشجو تأیید می‌نماید که مطالب مندرج در این پایان‌نامه نتیجه تحقیقات خودش می‌باشد و در صورت استفاده از نتایج دیگران مرجع آن را ذکر نموده است.

سمانه خالقی

تاریخ و امضاء

1396/6/6

این جانب سمانه خالقی دانشجوی ورودی سال 1394 مقطع کارشناسی ارشد رشته الهیات گرایش فقه و مبانی حقوق اسلامی گواهی می‌نمایم چنانچه بر اساس مطالب پایان‌نامه خود اقدام به انتشار مقاله، کتاب و... نمایم ضمن مطلع نمودن استاد راهنما، با نظر ایشان نسبت به نشر مقاله، کتاب و... و به صورت مشترک و با ذکر نام استاد راهنما مبادرت نمایم.

سمانه خالقی

تاریخ و امضاء

1396/6/6

کلیه حقوق مادی مترتب از نتایج مطالعات، آزمایش‌ها و نوآوری ناشی از تحقیق موضوع این پایان‌نامه متعلق به دانشگاه پیام نور می‌باشد.

تابستان 1396

به مصداق "من لم يشكر
المخلوق لم يشكر الخالق"
بسی شایسته است از اساتید
فرهیخته و فرزانه
سرکار خانم دکتر گواهی و
جناب آقای دکتر کریمی
که با کرامتی چون
خورشید، سرزمین دل را روشنی
بخشیدند و گلشن سرای علم و
دانش را با راهنمایی های کار
ساز و سازنده بارور
ساختند؛ تقدیر و تشکر نمایم.

تقدیم

ماحصل آموخته‌هایم را تقدیم می‌کنم به
آنان که مهر آسمانی‌شان آرام‌بخش آلام
زمینی‌ام است؛
به روح پر فتوح پدرم،
به زیباترین نگاه زندگی‌ام، چشمان زیبای
مادرم
همسرم، برای تمام محبت‌ها و فداکاریهایش

بسمه تعالی

نام خانوادگی: خالقی	نام: سمانه
عنوان پایان نامه: بررسی فقهی حقوقی هکرهای سایبری در حوزه پول و معاملات اقتصادی	
استاد راهنما: دکتر زهرا گواهی	استاد مشاوره: دکتر مهدی کریمی
نماینده گروه آموزشی: دکتر اعظم امینی	استاد داور: دکتر محسن لعل علیزاده

درجه تحصیلی: کارشناسی ارشد	رشته: الهیات	گرایش: فقه و مبانی حقوق اسلامی
دانشگاه: پیام نور	مرکز: مشهد	تاریخ دفاع: 96/6/27
.....		
تعداد صفحه:		
کلید واژه ها: سرقت، سرقت رایانه ای، هک کردن، داده و اطلاعات، تعزیر		
چکیده:		
<p>در تمامی کشورها، تنها اموری جرم است که طبق قوانین جاری آن کشور ارتکاب یا ترک آن جرم به حساب آید که سرقت رایانه ای و هک کردن نیز از این قاعده مستثنی نیستند. سرقت رایانه ای و هک کردن توسط هکرها یکی از مصادیق جرایم رایانه ای است که در فضای اینترنتی ارتکاب می یابد. امروزه در اکثر کشورهای جهان به عنوان یک عمل مخالف قانون به رسمیت شناخته شده و برای مرتکبین آن مجازات در نظر گرفته شده است. سرقت رایانه ای در واقع دسترسی پیدا کردن غیر مجاز به داده های دیگری و ربودن یا انتقال آن می باشد که در این پژوهش با توجه به قانون ایران این جرم رایانه ای مورد مطالعه قرار گرفته است.</p> <p>تفاوت اساسی سرقت رایانه ای با سرقت های سنتی نه تنها در وسیله و ابزار ارتکاب جرم بلکه موضوع شان هم متفاوت است. موضوع سرقت رایانه ای داده و اطلاعات است که پدیده مذکور اعم از مال و غیر مال می باشد. پس با توجه به اینکه سرقت، ربودن مال دیگری به طور پنهانی است، از این رو ربودن داده های رایانه ای به طور مخفیانه سرقت رایانه ای می باشد، اما به دلیل حکومت قاعده درء، نمی توان مجازات قطع ید را برای سارق رایانه ای در نظر گرفت، هر چند داده ها به طور پنهانی ربوده شده باشند. اکثر فقهای معاصر نیز همین نظر را برگزیده اند. قانون جرایم رایانه ای نیز هر دو فرض سرقت رایانه ای را مستوجب تعزیر می داند. در این پروژه بعد از فصل اول که کلیات می باشد، در فصل دوم مفهوم شناسی بررسی شده و در فصل سوم سرقت در فقه و حقوق موضوعه مورد بررسی قرار گرفت، در فصل چهارم احکام فقهی و حقوقی سرقت را بر هک کردن هکرها بررسی نمودیم، تطبیق قواعد فقهیه بر هک کردن هکرها در فصل پنجم مورد بررسی قرار گرفت و در فصل ششم حفظ حریم خصوصی و هک کردن مورد بررسی قرار گرفت.</p>		

فهرست مطالب

1	فصل اول: کلیات
2	بیان مساله
4	اهمیت و ضرورت تحقیق
4	کاربردهای متصور از تحقیق
4	سابقه و پیشینه تحقیق
5	اهداف تحقیق
5	هدف اصلی
5	هدف فرعی
5	فرضیه ها
6	سئوالات مورد تحقیق
6	جنبه نوآوری و جدید بودن
6	روش انجام تحقیق
6	روش و ابزار گردآوری اطلاعات
6	قلمرو تحقیق از ابعاد موضوعی، زمانی، مکانی
7	فصل دوم: مفهوم شناسی موضوع
8	بخش اول: تعاریف علمی
8	گفتار اول: تعریف فضای مجازی
8	گفتار دوم: تعریف فضای سایبری
9	گفتار سوم: تعریف هک و هکر
10	مبحث اول: مفهوم هکر
11	مبحث دوم: برخی از اصطلاحات رایج در دنیای هک
11	مبحث سوم: اهداف حمله کننده ها
12	بخش دوم: انواع هکرها
12	1- هکرها سرخوش
12	2- هکرها امنیت کامپیوتر

12	3- کلاه سفیدها
12	4- کلاه سیاه ها
12	5- کلاه خاکستریها
12	6- فعالین هکری
13	7- اسکرپیت بازها
14	فصل سوم: سرقت در فقه و حقوق موضوعه
15	بخش اول: سرقت در فقه
15	گفتار اول: تعریف سرقت
15	مبحث اول: معنای لغوی سرقت
15	مبحث دوم: معنای اصطلاحی سرقت
15	مبحث سوم: تعریف فقهی سرقت
16	گفتار دوم: سرقت از دیدگاه آیات
17	گفتار سوم: سرقت از دیدگاه روایات
18	گفتار چهارم: جرم سرقت در منابع فقهی
19	بخش دوم: سرقت در حقوق موضوعه
19	گفتار اول: سرقت از دیدگاه حقوقی
20	گفتار دوم: جرم سرقت در منابع حقوقی
22	1- تجزیه و تحلیل جرم دزدی در قانون مجازات اسلامی
23	2- تجزیه و تحلیل ماده 665 قانون مجازات اسلامی
25	گفتار سوم: احکام سرقت
25	مبحث اول: احکام فقهی
26	مبحث دوم: احکام حقوقی
27	مبحث سوم: شرایط اجرای حد
27	مبحث چهارم: حد سرقت
30	فصل چهارم: تطبیق احکام فقهی حقوقی سرقت بر هک کردن در فضای اینترنتی
31	بخش اول: سرقت رایانه ای در قانون ایران
31	گفتار اول: مفهوم کلی سرقت رایانه ای
32	مبحث اول: شرایط تحقق سرقت

- 1- ربایش 32
- 2- قراردادن در حرز 33
- 3- مخفیانه بودن 35
- 4- مالیت داشتن شیء مسروقه 36
- 5- تعلق مال به غیر 37
- گفتار دوم: تعریف سرقت رایانه ای 39
- مبحث اول: سرقت رایانه ای (سرقت و تکثیر غیر مجاز برنامه های کامپیوتری حمایت شده) 39
- مبحث دوم: شرایط سرقت رایانه ای 42
- مبحث سوم: چگونگی انجام سرقت رایانه ای 43
- بخش دوم: عناصر مشکله سرقت رایانه ای 44
- گفتار اول: عنصر قانونی 45
- گفتار دوم: عنصر مادی 45
- گفتار سوم: عنصر روانی (معنوی) 47
- گفتار چهارم: انگیزه های هکرها 48
- گفتار پنجم: آیا میتوان به هکرها عنوان سارق را اطلاق کرد؟ 48
- بخش سوم: آرای فقهای معاصر 49
- فصل پنجم: تطبیق قواعد فقهیه بر هک کردن هکرها 53
- بخش اول: قاعده تسلیط 54
- گفتار اول: مستندات فقهی قاعده تسلیط 54
- گفتار دوم: نقش قاعده تسلیط در سرقت اینترنتی و هک کردن هکرها 60
- بخش دوم: قاعده لاضرر 61
- گفتار اول: مفهوم شناسی قاعده لاضرر 62
- مبحث اول: دلالت قاعده 62
- مبحث دوم: تبیین قاعده "لاضرر" و تقسیم آن به مادی و معنوی با محوریت ضرر معنوی 63
- گفتار دوم: مستندات فقهی قاعده "لاضرر" 63
- گفتار سوم: نقش قاعده لاضرر در سرقت اینترنتی و هک کردن هکرها 65
- بخش سوم: قاعده اکل مال بالباطل 65
- گفتار اول: مبنای جرم 65

66	مبحث اول: دیدگاه اول (دیدگاه فقهی)
68	مبحث دوم: دیدگاه دوم (دیدگاه حقوقی)
69	گفتار دوم: عناصر رکن مادی جرم
69	مبحث اول: مرتکب جرم
70	مبحث دوم: رفتار مجرمانه مرتکب
71	مبحث سوم: موضوع جرم
72	گفتار سوم: نامشروع بودن تحصیل مال
73	گفتار چهارم: تفویض اختیار از سوی دولت
74	گفتار پنجم: رکن روانی جرم
76	گفتار ششم: نقش قاعده اکل مال بالباطل در سرقت اینترنتی
76	گفتار هفتم: تعریف کلاهبرداری اینترنتی
78	فصل ششم: حفظ حریم خصوصی و هک کردن
79	بخش اول: تعریف حریم خصوصی
79	گفتار اول: مصادیق حریم خصوصی
79	مبحث اول: حریم اطلاعات و حریم ارتباطات
80	مبحث دوم: نظرات موافقین و مخالفین حریم خصوصی در فضای مجازی
81	مبحث سوم: فضای مجازی منکر حریم خصوصی است
81	مبحث چهارم: نحوه حمایت از حریم خصوصی اطلاعات شخصی در حقوق ایران
82	مبحث پنجم: انتقادات وارد بر نظام حقوقی ایران در زمینه حمایت از حریم خصوصی اطلاعات شخصی
83	مبحث ششم: تلفن همراه حریم شخصی نیست
84	بخش دوم: نقض حریم خصوصی در فضای مجازی و مجازات های آن
84	گفتار اول: نقض حریم خصوصی در فضای مجازی
85	گفتار دوم: بررسی عواقب جرم در فضای مجازی از نگاه قانون
87	گفتار سوم: مقایسه حریم خصوصی با حرز
88	نتیجه گیری
89	پیشنهادها
90	منابع و مآخذ

فصل اول

کلیات

بیان مسأله

فضای سایبری در معنا به مجموعه ای از ارتباطات درونی انسانها از طریق کامپیوتر و مسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می شود، در نتیجه یک سیستم آنلاین یا یک تلفن همراه یا یک دستگاه خود پرداز نمونه ای از فضای سایبر است که کاربران آن می توانند از طریق آن با یکدیگر ارتباط برقرار کنند. جرایم سایبری به دو بخش تقسیم می شوند:

- 1- جرائمی که در آن خود کامپیوتر مورد هدف قرار می گیرد و یا جرائم کامپیوتری.
- 2- جرائمی که در آن از کامپیوتر به عنوان ابزاری برای ارتکاب به یک جرم سنتی استفاده می شود یا جرائم مرتبط با کامپیوتر.

جرائم کامپیوتری شامل اقداماتی برای صدمه وارد کردن و یا دزدیدن اطلاعات کامپیوتر می باشد که "هک کردن" را می توان به عنوان مهمترین و معروف ترین نمونه برای جرم کامپیوتری مثال زد، در توضیح اقدام هکرها می توان گفت که افراد مذکور بدون اجازه و با پیدا کردن یک راه پنهانی در کامپیوتر شخصی یک فرد دیگر به جستجو پرداخته و اطلاعات آن را دزدیده و یا تغییر می دهند.

مباحث مربوط به جرایم رایانه ای بر خلاف جرایمی که ماهیت سنتی دارند و مبانی آنها طی قرون و اعصار شکل گرفته و ابعاد آن روشن شده، چند دهه پیشتر نیست که مطرح شده است. از این رو مسائل جدید و ناگفته در این زمینه بسیار زیاد می باشد. رایانه به موازات خدمات بی شمار خود، همچون دیگر دستاورد های علمی و صنعتی، امکان بهره بردن نادرست از آن و تبدیل شدن به ابزاری برای ارتکاب جرم و بزه را داراست. از جمله جرایمی که از طریق رایانه امکان دارد سرقت و من جمله هک کردن توسط هکرها می باشد که با تعبیری همچون سرقت رایانه ای، سرقت اینترنتی و سرقت در فضای مجازی یا سایبر معروف و مشهور می باشد.

سرقت از جمله جرایمی است که از همان اعصار کهن، از آن به عنوان یک پدیده زشت و ناپسند یاد شده است. تمامی ادیان، سرقت را عملی مردود دانسته و برای مرتکب آن مجازات در نظر گرفته اند. در دین مبین اسلام نیز، سرقت حرام شمرده شده است. این موضوع از ضروریات دین اسلام محسوب می شود و مبانی و ریشه های آن در ادله اربعه (کتاب، سنت، اجماع و عقل) موجود است.

در فقه و حقوق اسلام کیفر جرم سرقت قطع دست می باشد که منوط به احراز شرایط خاصی می باشد. امروزه با ورود رایانه ها و شبکه های رایانه ای شیوه وقوع و ماهیت این جرم تغییر پیدا کرده است. این تغییر و تحول باعث نگرانیهای زیادی برای مردم و موسسات مالی و اعتباری شده است، چرا که سرقت مقادیر زیادی پول و اعتبار در کوتاهترین زمان ممکن و به راحتی قابل انجام است. همین عامل باعث شده میزان ارتکاب این جرم در فضای مجازی روز به روز افزوده شود.

از این رو می بایست مسائل فقهی و حقوقی آن به طور جدی مورد مطالعه و بررسی قرار گیرد تا بتوان در حد امکان امنیت و نظم را در فضای مجازی ایجاد کرد.

در این پژوهش هدف از هک کردن و سرقت، سرقتی است که توسط کامپیوتر یا اینترنت و در محیط اینترنتی یا فضای سایبری صورت می گیرد نه سرقتی که علیه کامپیوتر یا رایانه می باشد.

اختصاص و توجه این پروژه به مفهوم و ماهیت سرقت و تطبیق احکام فقهی حقوقی آن بر هک کردن در فضای مجازی می باشد و همچنین تطبیق قواعد فقهیه بر هک کردن هکرها از مباحث دیگر این پروژه می باشد. پرسش اساسی که مطرح می شود این است که، شرایط تحقق سرقت رایانه ای (کامپیوتری) و چگونگی انجام آن چه بوده و تفاوت آن با سرقت عادی چیست؟ و اینکه آیا فضای مجازی حریم خصوصی محسوب می شود یا نه؟ لذا پژوهش حاضر در پی حل مسأله و پاسخگویی به پرسشهای فوق می باشد.

اهمیت و ضرورت تحقیق

امروزه بسیاری از مردم از شبکه جهانی یا اینترنت برای مبادله پیام یا فعالیتهای دیگر استفاده می کنند. این شبکه ها فاصله زمانی و مکانی را از بین برده و قدرت زیادی در اختیار بشر قرار داده است، چون این فناوری فضای اشتراکی ایجاد کرده و مفاهیم جدیدی چون حاکمیت سایبری و... را به منصف ظهور رسانده است، از طرفی این فضا شرایط سوء استفاده را برای افراد بزهکار فراهم کرده است، از این روی در این فضا نیز ممکن است انسان مرتکب جرم شود.

چون چنین جرمی در فضای اینترنتی روی می دهد آن را جرم الکترونیکی یا سایبری نام می نهند. لذا برای مقابله با چنین جرایم و سوء استفاده از آن نیازمند تدوین قوانین جدیدی هستیم که حقوق سایبری نام دارد.

کاربرد های متصور از تحقیق

هدف کاربردی و اساسی این پروژه شامل تقویت دستگاه قضایی و ظرفیت های اجرایی قانونی کشور در رابطه با جرایم سایبری، تهیه آماری در مورد وقوع این جرایم در کشور، توسعه یک مکانیسم پاسخگویی ایده آل به این جرایم و سرانجام ارتقا، آگاهی عمومی از جرایم سایبری در میان جمعیت کاربر اینترنت می باشد.

سابقه و پیشینه تحقیق

در این زمینه کار پژوهشی زیاد به نظر نمی رسد تنها بعضی از پژوهش های مربوط به خود جرایم رایانه ای از منظر فقهی و حقوقی می باشد. اما در زمینه جرایم در محیط مجازی و سایبری می توان به جزوه آموزشی جرایم سایبر یا گزیده های اخبار جرایم سایبری توسط محمد حسن دزیانی اشاره کرد. همچنین کتابی با عنوان بررسی فقهی حقوقی جرایم رایانه ای توسط حسینعلی بای و بابک پور قهرمان نگاشته شده که به جرایم ارتكابی از طریق رایانه در محیط مجازی و سایبری می پردازد.

و شاهین دژ هم در پژوهش خود با عنوان ماهیت فقهی و حقوقی سرقت الکترونیکی این تحقیق را انجام داد و به نتایج زیر دست یافت:

سرقت الکترونیکی نیز مثل سرقت های سنتی و عادی مشمول تعریف سرقت است و احکام سرقت عادی بر سرقت الکترونیکی نیز تسریع دارد.

جرم سرقت الکترونیکی نیز مثل سایر جرایم رایانه ای و اینترنتی دارای عنصر مادی خاص خود می باشد و کلیه مراحل رایانه و اینترنت قابلیت آن را دارند که مورد فعالیت مجرمانه قرار گیرند.

در عنصر روانی یا معنوی جرم، عمل مجرمانه باید ماحصل نیت و اراده مجرم باشد، به عبارت دیگر میان عمل مادی و حالات روانی مرتکب باید ارتباطی وجود داشته باشد تا مرتکب مقصر شناخته شود. (شاهین دژ، 1391، شماره 12 و 13)

اهداف تحقیق

هدف اصلی:

مهمترین هدف از انجام این تحقیق چگونگی انجام جاسوسی رایانه ای و حل مشکلات و موانع برای مقابله با آنهاست. با توجه به اینکه پیشرفت‌ها در فضای سایبری لحظه به لحظه و روز به روز بیشتر است باید قانونی داشته باشیم جامع و در عین حال منعطف که به صورت دایره ای بتوان آن را مورد تجدید نظر قرار داد و یا قانون گذار در این قانون دست مجریان را برای تطبیق موضوعات جدید با احکام قانونی باز بگذارد زیرا نمی توان خارج از چارچوب قانون حرکت کرد، قانون باید جامع و قدرت باز دارندگی کافی داشته باشد تا بتوان از سوء استفاده های افراد سود جو مثل هک کردن یک سایت و دسترسی غیر مجاز به اطلاعات یک موسسه یا یک خانواده از طریق اینترنت جلوگیری کرد.

هدف فرعی:

در این تحقیق سعی می شود با رویکردی پیش برود که بتواند به دستگاههای قضایی کمک نماید.

فرضیه ها

- 1- به کسی که عمل هک را انجام می دهد هکر گویند و هکرها با داشتن زبان برنامه نویسی به یک سیستم رایانه ای نفوذ می کنند.
- 2- قانون مجازات اسلامی برای هکرها حکم تعزیر در نظر گرفته است.
- 3- دستگاه اجرایی و قانون کنترل و شناسایی هکرها در جمهوری اسلامی پلیس فتا می باشد.
- 4- احکام فقهی حقوقی سرقت بر هک کردن نیز منطبق می شود.
- 5- احکام قواعد فقهیه بر هک کردن نیز منطبق می شود.

سؤالات مورد تحقیق

- 1- هکرها به چه کسانی گفته می شود؟
- 2- قانون مجازات اسلامی چه مجازاتی برای هکرها تدوین نموده است؟
- 3- دستگاه اجرایی و قانونی کنترل و شناسایی هکرها در جمهوری اسلامی چیست؟

4- احکام فقهی حقوقی سرقت چگونه بر هک کردن تطبیق می شود؟

5- قواعد فقهیه چگونه بر هک کردن تطبیق می شود؟

جنبه نوآوری و جدید بودن

این موضوع به ویژه به طور جزئی تر در حوزه پول و معاملات اقتصادی از نوآوری برخوردار می باشد.

روش انجام تحقیق

روش اجرای تحقیق به صورت توصیفی - تحلیلی می باشد که تلاش می کند به بررسی هک‌های اینترنتی و سایبری در حوزه پول و معاملات اقتصادی بپردازد.

روش و ابزار گردآوری اطلاعات

روش و ابزار گردآوری به شکل کتابخانه ای می باشد و با استفاده از کتابها، سایتها، مشاهده و کمک از مقالات معتبر می باشد.


قلمرو و تحقیق از ابعاد موضوعی، زمانی، مکانی

از نظر موضوعی:

این پژوهش از دو حوزه دانش فقه و حقوق به بررسی موضوع خواهد پرداخت.

از نظر مکانی و زمانی:

قوانین کشور جمهوری اسلامی ایران مد نظر می باشد.



فصل دوم

مفهوم شناسی

موضوع

بخش اول: تعاریف علمی

گفتار اول: تعریف فضای مجازی

در تمام تعاریف فضای مجازی، این فضا محیط الکترونیکی یا محیط شبکه ای از کامپیوتر ها دانسته می شود که با استفاده از جلوه های سمعی و بصری سعی دارد تا اشیاء و واقعیت های سه بعدی جهان واقعی را مشابه سازی کند، اما ادعا می شود که فاقد مادیت فیزیکی هستند.

گفته می شود که از خصوصیات بارز این فضا بی مکانی و بی زمانی است. اما کار واژه سایبر، از ریشه یونانی لغت کنترل گرفته شده و به طور ترکیبی در واژه سایبرنتیک به کار رفته است.

مفهوم سایبرنتیک دلالت بر سیستم های کنترلی ابر تکنولوژی های رایانه های به هم پیوسته، تکنولوژی جدید و واقعیات مصنوعی با راهبردهای دستیابی و کنترل سیستمی دارد.

مفهوم فضا معمولاً در مقایسه با مفهوم مکان توصیف و تعریف می شود و بدون شک نخستین وجه تمایزی که در جریان مقایسه مکان و فضا برجسته است، سطح انتزاع این دو مفهوم است.

همچنین فضای مجازی را می توان برای توصیف تمام انواع اطلاعاتی موجود شده از طریق شبکه های رایانه ای به کار برد، در حقیقت فضای مجازی نوع متفاوتی از واقعیت مجازی و دیجیتالی است که توسط شبکه های رایانه ای هم پیوند تامین می شود که با اندکی مسامحه می توان آن را مترادف با شبکه جهانی اینترنت دانست.

گفتار دوم: تعریف فضای سایبری:

فضای سایبر (Cyberspace) عبارتی است که در دنیای اینترنت، رسانه و ارتباطات بسیار شنیده می شود. به نظر می رسد به کارگیری این اصطلاح در این زمینه و برای ارجاع به امور فنی به آن رنگ و بویی صرفاً فنی و مکانیکی داده باشد. ملاحظه دقیق تر این اصطلاح نشان می دهد که این واقعیت، وجوه و جنبه های متنوعی از جمله خصلت های روانشناختی قابل توجه نیز دارد.

در منابع موجود آمده است که:

واژه سایبر از لغت یونانی Kybernetes به معنی سکاندار یا راهنما مشتق شده است. نخستین بار این اصطلاح "سایبرنتیک" توسط ریاضیدانی به نام نوربرت وینر Norbert Wiener در کتابی با عنوان "سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین" در سال 1948 بکار برده شده است.

سایبرنتیک علم مطالعه و کنترل مکانیزم ها در سیستم های انسانی، ماشینی (و کامپیوتر ها) است. سایبر پیشوندی است برای توصیف یک شخص، یک شی، یک ایده و یا یک فضا که مربوط به دنیای کامپیوتر و اطلاعات است.

واژه "فضای سایبر" را نخستین بار ویلیام گیسون William Gibson نویسنده داستان علمی تخیلی در کتاب

نورومنس Neuromancer در سال 1984 به کار برده است. فضای سایبر در معنا به مجموعه هایی از ارتباطات درونی انسانها از طریق کامپیوتر و مسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می شود. یک سیستم آنلاین نمونه ای از فضای سایبر است که کاربران آن می توانند از طریق ایمیل با یکدیگر ارتباط برقرار کنند.

برخلاف فضای واقعی، در فضای سایبر نیاز به جابجایی های فیزیکی نیست و کلیه اعمال فقط از طریق فشردن کلیدهای حرکات ماوس صورت می گیرد.

این عدم جابجایی فیزیکی، محققان را واداشت که به مطالعه برخی شباهت های فضای سایبر با حالت های نا هشیاری، به خصوص حالت های ذهنی ای که در رویا ها ظاهر می شوند، بپردازند.

در واقع می توان گفت که فضای سایبر گستره ای از ذهن است که می تواند تمامی اشکال زندگی منطقی را بسط و معنا دهد. شما می توانید حالت های متنوع و متفاوت ذهنی را از قبیل تخیلات (خیال پردازی ها) خیالپروریها، توهمات، حالات هیپنوتیستیک و سطوح گوناگونی از هوشیاری را در فضای مجازی تجربه کنید. تحت این چنین شرایط است که فضای سایبر همانند دنیای "رویا" می شود. دنیایی که وقتی ما به خواب فرو می رویم، پدیدار می شود.

فضای سایبر را نمی توان تنها یک "بزرگ شاهراه اطلاعاتی" ساده دانست. زیرا تجربه ذهنی ما در فضای مجازی با تجربه ذهنی ما زمانی که بی هیچ هدف و ارزشی خیال بافی می کنیم، کاملاً متفاوت است.

در واقع همان گونه که علم روانشناسی خواب شبانه را برای حفظ سلامتی، توسعه عاطفی و رشد شخصیت یک فرد ضروری می داند، این فضای مجازی هم بیش از هر چیز دیگری در خدمت روان انسان است. زیرا مرزهای بین واقعیت های آگاهانه و نا آگاهانه را به هم نزدیک ساخته و می تواند درباره معنای "واقعیت" چیز هایی به ما بگوید.

گفتار سوم: تعریف هک و هکر

هک یکی از واژه هایی است که در سال های اخیر به وفور شنیده شده است و هر روز خبر هایی از حملات هکری گروه ها و یا افرادی را می شنویم که به دلایل مختلف از جمله خرابکاری و یا هشدار امنیتی و اعتراض و ... دست به این کار می زنند.

دنیای تکنولوژی هر لحظه در حال پیشرفت است و با پیدایش یک صنعت یا علم جدید بلافاصله محصولی علیه آن عرضه می شود. با پیشرفت دنیای کامپیوترها و آغاز نسل اول ارتباط های شبکه ای کم کم نفوذ و هک شکل گرفت.