

بسم الله الرحمن الرحيم



دانشکده معارف اسلامی و حقوق

پایان نامه کارشناسی ارشد رشته معارف اسلامی و حقوق گرایش حقوق جزا و جرم‌شناسی

سیاست کیفری ایران در قبال هک

استاد راهنما: دکتر طاهر حبیب زاده

استاد مشاور: دکتر سلمان عمرانی

دانشجو: علیرضا صفدری

شهریور ۱۴۰۱

کلیه حقوق اعم از چاپ و تکثیر، نسخه‌برداری، ترجمه، اقتباس و نظایر آن‌ها از این «پایان‌نامه‌ی کارشناسی ارشد» برای دانشگاه امام صادق «علیه‌السلام» محفوظ است. نقل مطالب با ذکر ماخذ بلامانع است.

خداوند متعال را بابت اعطای فرصت کسب علم شاکرم.

از اساتید گرانقدر دکتر طاهر حبیب‌زاده و دکتر سلمان عمرانی بابت راهنمایی و مشاوره این اثر
تشکر میکنم.

چکیده

با گسترش فناوری‌های نوین در سال‌های اخیر جرایم هم شکل تازه‌ای به خود گرفته‌اند و جامعه‌ی حقوقی را با مسائل نو و بدیعی مواجه ساخته‌است، مسائلی که اگر به موقع به آن‌ها پاسخ داده نشود ممکن است باعث خسارات بسیار بزرگ به دولت و جامعه شود، مسائلی مانند هوش مصنوعی، بلاکچین و رمزارزها، ربات‌ها، دارکوب، اینترنت اشیا، دولت الکترونیک و ...، رویکرد قانون‌گذار ایران نسبت به این مسائل چیست؟ در این پژوهش سعی شده‌است با نگاه کمی عمیق‌تر به جنبه‌های فنی این مسائل، ابعاد بیشتری از آن‌ها را برای سایر پژوهشگران باز کرده تا اولاً ضعف‌های قوانین فعلی آشکار شود، ثانیاً فضای جرایم سایبری و ابعاد فنی آن برای حقوق‌دانان واضح‌تر شود و ثالثاً راهکارهایی برای سیاست‌گذاری و قانون‌گذاری در این حوزه ارائه شود.

کلمات کلیدی: جرم رایانه‌ای، سیاست کیفری، هک

فهرست مطالب

مقدمه	۱۰
۱. بیان مساله	۱۰
۲. اهمیت و ضرورت	۱۳
۳. سوالات و فرضیه‌های پژوهش	۱۴
۴. شیوه انجام پژوهش	۱۴
۵. پیشینه پژوهش	۱۵
۱.۵. کتاب جرایم رایانه‌ای	۱۵
۲.۵. کتاب درآمدی بر آیین دادرسی کیفری جرایم سایبری	۱۵
۳.۵. کتاب پی‌جویی جرایم رایانه‌ای	۱۵
۴.۵. پایان‌نامه بررسی حقوقی و فقهی هک	۱۶
۵.۵. پایان‌نامه بررسی فقهی حقوقی هک‌های سایبری در حوزه پول و معاملات اقتصادی	۱۶
۶.۵. پایان‌نامه بررسی فقهی حقوقی جرایم سایبری	۱۶
۷.۵. رساله سیاست کیفری افتراقی در جرایم سایبر با تأکید بر حقوق کیفری ایران	۱۶
۸.۵. بازمهندسی قواعد تعیین صلاحیت قضایی در جرایم اینترنتی	۱۶
۹.۵. مقاله اصول جرم‌انگاری در فضای سایبر	۱۷
۱۰.۵. مقاله راهکارهای مقابله با کلاهبرداری رایانه‌ای	۱۷
۶. جنبه نوآوری پژوهش	۱۷
۷. بخش‌های پژوهش	۱۷

۱۸	پیشینه، مفاهیم و مبانی	۱
۱۸	پیشینه	۱.۱
۱۸	سطح بین‌المللی	۱.۱.۱
۱۹	گروه G8	۱.۱.۱.۱
۱۹	سازمان ملل	۲.۱.۱.۱
۱۹	سازمان همکاری‌های اقتصادی آسیا-پاسفیک	۳.۱.۱.۱
۱۹	شورای اروپا	۴.۱.۱.۱
۲۰	اتحادیه کشورهای مشترک‌المنافع	۵.۱.۱.۱
۲۰	اتحادیه اروپا	۶.۱.۱.۱
۲۰	ایالات متحده	۷.۱.۱.۱
۲۱	چین	۸.۱.۱.۱
۲۱	ایران	۲.۱.۱
۲۲	قانون جرایم نیروهای مسلح	۱.۲.۱.۱
۲۲	قانون تجارت الکترونیکی	۲.۲.۱.۱
۲۲	قانون جرایم رایانه‌ای	۳.۲.۱.۱
	قانون آیین دادرسی جرایم نیروهای مسلح و دادرسی	۴.۲.۱.۱
۲۳	الکترونیکی	
۲۳	مفاهیم	۲.۱
۲۳	سیاست کیفری	۱.۲.۱
۲۳	جرم رایانه‌ای	۲.۲.۱
۲۴	computing device	۱.۲.۲.۱
۲۴	network	۲.۲.۲.۱
۲۵	هک	۳.۲.۱
۲۶	مراحل هک	۴.۲.۱
۲۷	اجزای امنیت اطلاعات	۵.۲.۱
۳۰	دفاع در عمق	۶.۲.۱
۳۰	لایه‌های اینترنت	۷.۲.۱
۳۲	دارک وب	۸.۲.۱

۳۳	شبکه تور	۹.۲.۱
۳۴	سیستم عامل tails و کالی لینوکس	۱۰.۲.۱
۳۴	رمزارز	۱۱.۲.۱
۳۵	هوش مصنوعی	۱۲.۲.۱
۳۵	مبانی	۳.۱
۳۵	صلاحیت محاکم ایران در جرایم رایانه‌ای	۱.۳.۱
۳۹	مسئولیت کیفری انواع هکر	۲.۳.۱
۳۹	هکر کلاه سیاه	۱.۲.۳.۱
۳۹	هکر کلاه سفید	۲.۲.۳.۱
۴۰	هکر کلاه خاکستری	۳.۲.۳.۱
۴۰	هک‌های انتحاری	۴.۲.۳.۱
۴۱	بچه‌اسکرپتی‌ها	۵.۲.۳.۱
۴۲	هک‌های حکومتی	۶.۲.۳.۱
۴۲	ربات‌ها	۷.۲.۳.۱

۴۶	جرایم علیه تمامیت داده و سامانه‌های رایانه‌ای	۲
۴۶	دسترسی غیرمجاز	۱.۲
۴۶	تعریف	۱.۱.۲
۴۷	مراحل	۲.۱.۲
۴۷	دسترسی پیدا کردن	۱.۲.۱.۲
۴۸	دزیده نگاه کردن	۱.۱.۲.۱.۲
۴۸	جستجو در زباله‌ها	۲.۱.۲.۱.۲
۴۸	حمله دیکشنری	۳.۱.۲.۱.۲
۴۹	حدس پسورد	۴.۱.۲.۱.۲
۴۹	حدس بر اساس اطلاعات بزه‌دیده	۵.۱.۲.۱.۲
۴۹	استفاده از کیلاگر	۶.۱.۲.۱.۲
۴۹	استفاده از بدافزارها	۷.۱.۲.۱.۲
۵۰	استفاده از usb	۸.۱.۲.۱.۲
۵۰	شنود کابلی	۹.۱.۲.۱.۲

۵۰	حمله واسطه شدن	۱۰.۱.۲.۱.۲	
۵۱	استفاده از شبکه	۱۱.۱.۲.۱.۲	
۵۱	replay attack	۱۲.۱.۲.۱.۲	
۵۱	روش های پیشگیری از پسورد کرکینگ	۱۳.۱.۲.۱.۲	
۵۲	افزایش سطح دسترسی	۲.۲.۱.۲	
۵۴	دو مساله فرعی	۳.۲.۱.۲	
۵۶	شنود اطلاعات	۲.۲	
۵۶	تعریف	۱.۲.۲	
۵۶	انواع روش ها	۲.۲.۲	
۵۶	شنود کابلی	۱.۲.۲.۲	
۵۷	شنود از طریق مک آدرس دستگاه ها	۲.۲.۲.۲	
۵۹	DHCP Starvation Attack	۳.۲.۲.۲	
۶۰	ARP Spoofing Attack	۴.۲.۲.۲	
۶۱	مهندسی اجتماعی	۳.۲	
۶۱	تعریف	۱.۳.۲	
۶۳	روش ها	۲.۳.۲	
۷۴	بدافزارها	۴.۲	
۷۴	کلیات	۱.۴.۲	
۷۴	تعریف بدافزار	۱.۱.۴.۲	
۷۵	انواع بدافزارها	۲.۱.۴.۲	
۷۵	تروجان	۱.۲.۱.۴.۲	
۷۵	ویروس	۲.۲.۱.۴.۲	
۷۷	کرم	۳.۲.۱.۴.۲	
۷۸	کی لاگر	۴.۲.۱.۴.۲	
۷۹	اجزای سازنده ی یک بدافزار	۳.۱.۴.۲	
۸۰	پیشینه	۲.۴.۲	
۸۲	عنصر مادی	۳.۴.۲	
۸۲	ساخت نرم افزار ساخت بدافزار	۱.۳.۴.۲	

۲.۳.۴.۲	ساخت بدافزار	۸۵
۳.۳.۴.۲	انتقال بدافزار به سیستم قربانی	۸۶
۴.۳.۴.۲	دسترسی به داده‌های خصوصی	۹۵
۵.۳.۴.۲	حذف یا تغییر داده‌های حیاتی سیستم‌عامل	۹۵
۶.۳.۴.۲	عکس‌برداری، ضبط فیلم و صدا از رایانه‌ی بزه‌دیده	۹۶
۷.۳.۴.۲	ارسال ایمیل‌های جعلی از طریق رایانه‌ی بزه‌دیده	۹۶
۸.۳.۴.۲	غیرفعال کردن تدابیر امنیتی مانند آنتی‌ویروس و دیوار آتش	۹۷
۹.۳.۴.۲	ایجاد دسترسی از راه دور	۹۷
۱۰.۳.۴.۲	ایجاد بک‌دور برای نفوذ بعدی	۹۷
۱۱.۳.۴.۲	سرقت اطلاعات بزه‌دیده مانند گذرواژه‌ها، اطلاعات کارت‌های بانکی و	۹۸
۱۲.۳.۴.۲	تخریب داده‌های بزه‌دیده	۱۰۱
۱۳.۳.۴.۲	رمزگذاری یا ایجاد مانع دسترسی بزه‌دیده به سیستم	۱۰۱
۱۴.۳.۴.۲	ایجاد شبکه‌ی ربانی	۱۰۱
۱۵.۳.۴.۲	استفاده از سیستم قربانی به عنوان پروکسی	۱۰۳
۱۶.۳.۴.۲	تغییر ظاهر گرافیکی	۱۰۳
۱۷.۳.۴.۲	کند شدن فعالیت‌های سامانه	۱۰۴
۱۸.۳.۴.۲	عدم نمایش برنامه‌ها	۱۰۴
۱۹.۳.۴.۲	تغییر عنوان فایل‌ها	۱۰۴
۲۰.۳.۴.۲	از کار افتادن سامانه	۱۰۴
۲۱.۳.۴.۲	تخریب داده‌ها	۱۰۴
۲۲.۳.۴.۲	نمایش پنجره‌های تبلیغاتی	۱۰۴
۴.۴.۲	مجازات	۱۰۵
۱.۴.۴.۲	تعدد جرم	۱۰۵
۱.۱.۴.۴.۲	تعدد نتیجه	۱۰۶
۲.۱.۴.۴.۲	تعدد مادی	۱۰۶
۳.۱.۴.۴.۲	تعدد معنوی	۱۰۶

۱۰۹	تشدید مجازات	۲.۴.۴.۲	
۱۱۱	تخریب منابع سرور یا حمله DOS	۵.۲	
۱۱۱	تعریف	۱.۵.۲	
۱۱۴	انواع	۲.۵.۲	
۱۱۴	UDP Flood attack	۱.۲.۵.۲	
۱۱۵	Permanent DoS	۲.۲.۵.۲	
۱۱۵	Destributed Denial of Service	۳.۲.۵.۲	
۱۱۸	حملات علیه وبسایت	۶.۲	
۱۱۸	تعریف	۱.۶.۲	
۱۱۹	انواع	۲.۶.۲	
۱۱۹	حمله DDoS	۱.۲.۶.۲	
۱۲۰	DNS Server Hijaching	۲.۲.۶.۲	
۱۲۰	Directory Traversal Attack	۳.۲.۶.۲	
۱۲۱	ربودن نشست‌ها	۴.۲.۶.۲	
۱۲۲	Man-in-the-Middle Attack	۵.۲.۶.۲	
۱۲۲	حمله فیشینگ	۶.۲.۶.۲	
۱۲۲	Website Defacement	۷.۲.۶.۲	
۱۲۳	حمله از طریق تزریق فایل	۸.۲.۶.۲	
۱۲۳	حمله به دلیل عدم وجود سطح دسترسی	۹.۲.۶.۲	
۱۲۳	حمله‌ی XSS	۱۰.۲.۶.۲	
۱۲۵	حمله‌ی csrf	۱۱.۲.۶.۲	
۱۲۵	تزریق داده	۷.۲	
۱۲۵	تعریف	۱.۷.۲	
۱۲۶	مراحل	۲.۷.۲	
۱۲۶	جستجوی آسیب‌پذیری‌ها	۱.۲.۷.۲	
۱۲۸	تزریق داده	۲.۲.۷.۲	
۱۳۰	حملات علیه وایرلس‌ها	۸.۲	
۱۳۰	تعریف	۱.۸.۲	

۱۳۰	انواع	۲.۸.۲
۱۳۱	ایجاد نقطه دسترسی جعلی	۱.۲.۸.۲
۱۳۱	حمله از طریق ضعف در پیکربندی دستگاه کاربر	۲.۲.۸.۲
۱۳۱	پیکربندی ضعیف نقطه دسترسی	۳.۲.۸.۲
۱۳۲	حمله‌ی ادهاک	۴.۲.۸.۲
۱۳۲	حمله‌ی نقطه دسترسی هانی پات	۵.۲.۸.۲
۱۳۳	حمله جعل هویت	۶.۲.۸.۲
۱۳۳	حمله‌ی DoS	۷.۲.۸.۲
۱۳۳	حمله‌ی key reinstallation	۸.۲.۸.۲
۱۳۴	ایجاد اختلال با پارازیت	۹.۲.۸.۲
۱۳۴	حملات علیه موبایل	۹.۲
۱۳۴	تعریف	۱.۹.۲
۱۳۴	انواع	۲.۹.۲
۱۳۴	اپلیکیشن‌های ناامن	۱.۲.۹.۲
۱۳۶	دسترسی‌های بیش از حد به موبایل	۲.۲.۹.۲
۱۳۶	اسمیشینگ	۳.۲.۹.۲
۱۳۷	حمله‌ی bluesnarfing و bluebugging	۴.۲.۹.۲
۱۳۷	حمله‌ی simjacker	۵.۲.۹.۲
۱۳۸	حملات علیه اینترنت اشیا	۱۰.۲
۱۳۸	تعریف	۱.۱۰.۲
۱۳۸	اجزای یک اینترنت اشیا	۱.۱.۱۰.۲
۱۳۹	کاربردهای اینترنت اشیا	۲.۱.۱۰.۲
۱۴۰	فناوری‌های مورد استفاده در اینترنت اشیا	۳.۱.۱۰.۲
۱۴۰	چالش‌های اینترنت اشیا	۴.۱.۱۰.۲
۱۴۱	انواع	۲.۱۰.۲
۱۴۲	DDoS Attack	۱.۲.۱۰.۲
۱۴۲	Exploit HVAC	۲.۲.۱۰.۲
۱۴۳	Rolling Code Attck	۳.۲.۱۰.۲

۱۴۴	BlueBorne Attack	۴.۲.۱۰.۲
۱۴۵	حملات مبتنی بر شنود امواج رادیویی	۵.۲.۱۰.۲
۱۴۶	حمله پارازیتی	۶.۲.۱۰.۲
۱۴۶	حمله از طریق دسترسی از راه دور به وسیله‌ی بک‌دور	۷.۲.۱۰.۲
۱۴۸	۳ جرایم به وسیله‌ی هک	
۱۴۸	۱.۳ جرایم علیه اشخاص	
۱۴۸	۱.۱.۳ استخدام قاتل	
۱۴۹	۲.۱.۳ مشارکت در اتاق قرمز	
۱۵۱	۳.۱.۳ قاچاق انسان و جرایم مرتبط	
۱۵۳	۱.۳.۱.۳ خرید و فروش اعضای بدن	
۱۵۴	۲.۳.۱.۳ بردگی جنسی	
۱۵۵	۴.۱.۳ جعل عمیق	
۱۵۵	۱.۴.۱.۳ سیاست	
۱۵۶	۲.۴.۱.۳ موارد غیراخلاقی	
۱۵۶	۵.۱.۳ آموزش‌های غیرمجاز	
۱۵۸	۲.۳ جرایم علیه اموال	
۱۵۸	۱.۲.۳ سرقت رایانه‌ای	
۱۵۸	۲.۲.۳ پولشویی	
۱۵۹	۳.۲.۳ اخاذی یا کلاهبرداری رایانه‌ای	
۱۶۰	۱.۳.۲.۳ روتون	
۱۶۰	۲.۳.۲.۳ کریپتو لاکر	
۱۶۱	۴.۲.۳ تخریب	
۱۶۲	۵.۲.۳ حضور در دارکوب و تاسیس فروشگاه	
۱۶۲	۳.۳ جرایم علیه امنیت و آسایش عمومی	
۱۶۲	۱.۳.۳ سایبرتروریسم	
۱۶۷	۲.۳.۳ جاسوسی رایانه‌ای	
۱۶۸	۳.۳.۳ خرید و فروش اقلام ممنوعه	

نتیجه‌گیری و پیشنهادات

۱۷۰

مقدمه

۱.۰ بیان مساله

روزبه‌روز با گسترش فناوری‌های نوین و افزایش نفوذ اینترنت بین مردم و همچنین ایجاد و گسترش دولت‌های الکترونیک در کشورها، گویی یک جهان موازی با این جهان غیرآنلاین ایجاد شده است، امور مالی از راه دور و از طریق بانک‌های اینترنتی انجام می‌شود، خدمات قضایی از طریق سامانه‌های اینترنتی ارائه می‌شود، صنایع و کارخانه‌ها اکثراً با سیستم‌های آنلاین و از راه دور کنترل می‌شوند، به زودی منازل مسکونی، فروشگاه‌ها و ... مجهز به اینترنت اشیاء^۱ شده و از راه دور کنترل می‌شوند، این تحولات قطعاً اقتضائات خاص خود را هم به همراه دارد.

نظام‌های حقوقی همواره در جریان تحولات فعال بوده و پاسخ‌هایی را به مسائل مستحدثه داده است، طبعاً انتظار می‌رود این بار هم این مسائل نوین به موقع بررسی شده و پاسخ‌های مناسب داده شود تا جامعه دوام داشته باشد و نظم آن حفظ شود.

تحولات نوین بسترهای نوینی برای ارتکاب جرم فراهم می‌کنند و طبیعتاً وقتی بسترهای ارتکاب جرم تغییر کند مجرمین هم تغییر می‌کنند، مجرمین دیگر افرادی پرزور نیستند که نهایتاً بتوانند در یک محله به ارتکاب قتل یا سرقت و ... بپردازند بلکه مجرمین جدید، افرادی بسیار باهوش و متخصص هستند که در کنج خانه‌ی خود بدون هیچ رد و نشانی در وسعت جهان به ارتکاب جرم می‌پردازند، هکرها مجرمین دنیای جدید هستند.

هک به معنای عام عبارتست از مجموعه اقداماتی که هکر انجام می‌دهد و هکر فردی است که تخصص بالایی در علوم رایانه مانند امنیت شبکه، نرم افزار، برنامه نویسی و ... دارد و از این دانش برای حمله به دیگران استفاده می‌کند.

از طرف دیگر سیاست کیفری عبارتست از مجموعه اقدامات کیفری و سرکوب‌گرایانه که توسط

¹internet of things(IOT)

دولت به معنای عام برای مدیریت جرم اتخاذ می‌شود، مشتمل بر جرم‌انگاری، مسئولیت کیفری و شدت کیفردهی. (مهر، ۱۳۹۷: ۵۳-۶۶)

بنابراین در این پژوهش به دنبال آن هستیم که مجموعه اقدامات حکومت در حوزه‌ی تقنین، قضا و اجرا را در موضوع هک و در سه حوزه‌ی جرم‌انگاری، مصادیق هک، مسئولیت کیفری هکرها و شدت کیفردهی بررسی کنیم.

۱. جرم‌انگاری

در قانون ایران، جرم مستقلی به نام هک وجود ندارد منتهی برخی مراحل هک به طور مستقل جرم‌انگاری شده‌است، قانون‌گذار ایران ابتدا در سال ۱۳۸۲ با تصویب قانون تجارت الکترونیکی و بعد در سال ۱۳۸۸ با تصویب قانون جرایم رایانه‌ای و ادغام آن با قانون مجازات اسلامی مصوب ۱۳۹۲ به جرم‌انگاری جرایم این حوزه پرداخته است و در سال ۱۳۹۴ با تصویب قانون آیین دادرسی کیفری، برخی مواد آن قانون را نسخ و رویکرد جدیدی در حوزه‌ی آیین دادرسی جرایم رایانه‌ای در پیش گرفته است.

قوانین مذکور از دو حیث ضعف دارند، نخست اینکه از زمان تصویب آن قانون تاکنون بیش از ۱۲ سال گذشته است و دنیای فناوری رایانه، دچار تحول‌های بسیار بزرگی در زمینه‌های مختلفی شده است، فناوری‌هایی مانند زنجیره بلوکی^۲، گسترش شبکه وب تاریک^۳، گسترش پردازش ابری^۴، روش‌های جدید رمزنگاری^۵، گسترش اینترنت اشیاء، رمزارزها^۶، داده‌کاو^۷، هوش مصنوعی^۸، یادگیری ماشینی^۹، یادگیری عمیق^{۱۰} و ... که هر کدام از اینها دنیایی از مسائل و چالش‌های جدیدی برای دولت‌ها ایجاد کرده‌اند و قانون‌گذار ایران در مورد این مسائل تاکنون منفعلانه رفتار کرده است و هیچ قانونی وجود ندارد.

دومین ضعف قوانین مذکور، عدم آشنایی دقیق و کامل قانون‌گذار نسبت به موضوع همان قانون است، گویی قانون‌گذار یک شبه و سیاهی‌ای از دور می‌دیده و مطابق همان تصور و برداشت خود از موضوع جرایم رایانه‌ای، اقدام به جرم‌انگاری کرده است، رویکرد فعلی

²blockchain

³Dark Web

⁴cloud computing

⁵cryptography

⁶cryptocurrency

⁷data mining

⁸artificial intelligence

⁹machine learning

¹⁰deep learning

نسبت به جرایم رایانه‌ای مانند این است که قانون‌گذار در جرم قتل عمد با چاقو این‌گونه جرم‌انگاری کند: تهیه چاقو یک‌سال حبس، پیدا کردن محل زندگی مجنی علیه یک‌سال حبس، زیر نظر گرفتن بزه‌دیده یک‌سال حبس، ورود به منزل بزه‌دیده یک‌سال حبس، داخل کردن چاقو در بدن یک‌سال حبس، از هاق نفس پنج سال حبس، ریختن خون روی زمین هم یک‌سال حبس! در خصوص جرایم سایبری الان دقیقاً اینگونه رفتار شده است؛ هکر در یک فرآیند هک، مجموعه اقداماتی را انجام می‌دهد تا به هدف خود برسد، قانون‌گذار الان تک تک کارهای هکر را جرم‌انگاری کرده است که اگر دقیق‌تر به مسائل این حوزه نگاه کنیم متوجه می‌شویم در عالم واقع برخی از این رفتارها تهیه وسایل و مقدمات جرم است، برخی در حد شروع به جرم، برخی فعل مادی جرم و برخی نتیجه جرم، منتهی قانون‌گذار به دلیل عدم شناخت دقیق این حوزه، همه‌ی این مراحل را به طور مستقل جرم‌انگاری کرده است که شاهد آن هستیم مجرمین با ارتکاب همه این جرایم در نهایت مشمول تعدد جرم شده و نسبت به مجازات استحقاقی و اثری که بر بزه دیده و جامعه می‌گذارد مجازات به مراتب خفیف‌تری را تحمل می‌کند.

۲. مسئولیت کیفری

در فرآیند هک ما با افراد مختلفی روبه‌رو هستیم که باید در خصوص مسئولیت کیفری آن‌ها بررسی‌ای صورت بگیرد؛ از حیث رکن معنوی اگر بخواهیم تقسیم‌بندی‌ای داشته باشیم، می‌توان به هکرهای کلاه سیاه، کلاه سفید، کارمندان و واسطه‌ها، ربات‌ها، مالکان پلتفرم‌ها و ... اشاره کرد که قانون‌گذار به طور مستقیم به این‌ها اشاره نکرده است منتهی مسئولیت کیفری برخی را می‌توان با مراجعه به قواعد عمومی حقوق و برخی را با مراجعه به منابع فقهی و فلسفی بررسی کرد که البته نیاز به تدقیق و پژوهش دارد.

۳. شدت کیفردهی

اگرچه قانون‌گذار هنوز تکلیفش با بسیاری از مسائل این حوزه مشخص نیست منتهی در همین حد ناقص، شاهد آن هستیم رویکرد فعلی قانون‌گذار در جرایمی که از طریق رایانه انجام می‌شود یک رویکرد افتراقی تشدید است، منتهی در خصوص هک هیچ رویکرد شفاف و یکپارچه‌ای نداریم و بعضاً میتوان از بررسی جرایم پراکنده‌ی رایانه‌ای مانند شنود رایانه‌ای، دسترسی غیرمجاز و ... حدس‌هایی زد، در هر حال باید به طور خاص بررسی شود

که آیا لازم است قانون‌گذار با توجه به وسعت اثرگذاری رفتارهای مجرمانه هکر، رویکرد خاصی نسبت به این مجرمین به طور مستقل اتخاذ کند یا خیر؟ پاسخ به این سوال نیاز به بررسی دقیق روح حاکم بر قوانین ایران و مراجعه به اصول و دکترین‌های حقوقی و همچنین بررسی مبانی فقهی دارد تا متناسب با ویژگی‌های جرایم رایانه‌ای یک سیاست کیفردهی مناسب پیشنهاد و اتخاذ شود.

۲.۰ اهمیت و ضرورت

به زودی در چند سال آینده با گسترش ۱۰۰ درصدی نسل‌های جدید اینترنت مانند 5G و بالاتر شاهد همه‌گیر شدن اینترنت اشیا در تمام نقاط شهرها و خانه‌ها هستیم، از طرف دیگر با راه‌اندازی دولت الکترونیک و اتصال همه سازمان‌ها و ادارات و کارخانه‌ها و ... به شبکه یکپارچه ابری، تهدیدات بالقوه‌ای در مقابل حکومت‌ها ایجاد می‌شود که عدم آمادگی در مقابل آن‌ها می‌تواند نه تنها باعث خسارت‌های هنگفت به اقتصاد آن حکومت شود بلکه امنیت سیاسی حکومت‌ها را هم تهدید می‌کند، آمادگی حکومت‌ها اعم است از آمادگی قوه مجریه، به عبارتی همه‌ی اجزای حکومت باید به طور هماهنگ برای سبک جدیدی از زندگی آماده شوند، از قوه مجریه که سکان‌دار اقتصاد و فرهنگ و ... است تا قوه مقننه که با وضع قوانین کامل می‌تواند ریل‌گذار این مسیر باشد و همچنین قوه قضاییه که محافظت از آن قوانین را بر عهده گرفته و متخلفان را به طور متناسب مجازات می‌کند.

لازمه‌ی وضع و اصلاح قوانین در حوزه جرایم رایانه‌ای، درک درست موضوع است، و این درک هم نیاز به پژوهشی عمیق و جامع و البته میان رشته‌ای بین رشته‌ی حقوق و رشته‌ی نرم‌افزار دارد، در همین راستا در این پژوهش به دنبال این هستیم که آخرین واقعیت‌های فنی حوزه امنیت و نفوذ سایبر را مطابق استانداردهای جهانی مانند CEH¹¹ در تمام مراحل هک بررسی کنیم، هم مصادیقی که هک در آن موضوعیت دارد مانند هک شبکه، سرور، وبسایت‌ها، موبایل، رایانش ابری، اینترنت اشیا و ... و هم مباحثی که هک به عنوان وسیله استفاده می‌شود مانند تروریسم سایبری¹²، جنگ سایبری¹³، پولشویی از طریق رمزارزها، معاونت در جرائم ارتكابی در بستر دارکوب مانند معاونت در قتل، آدم‌ربایی، تجاوز، فروش مواد مخدر و ... و در نهایت این مصادیق را با قوانین کیفری ایران سنجیده و از نظر حقوق کیفری و مسئولیت مدنی مورد بررسی قرار داده و در هر مرحله ببینیم کدام

¹¹ Certified Ethical Hacker

¹² cyberterrorism

¹³ cyberwar

مصادیق هک مطابق قوانین فعلی جرم است و کدام نیست؟ و از این طریق خلاءهای قانونی را پیدا و کارآمدی قوانین را بررسی کنیم.

و در نهایت خارج از قالب‌های پیشفرض قانون‌گذار در این حوزه، آنچه در عالم واقع از حیث جرم‌انگاری، مسئولیت کیفری و کیفردهی لازمه‌ی دوام و بقای جمهوری اسلامی در حوزه امنیت قضای سایبری است در قالب پیشنهاداتی ارائه دهیم و با بیان ساده‌تر و البته کامل‌تر مباحث تخصصی فنی این حوزه با ادبیات حقوقی، راه را برای سایر پژوهشگران این حوزه اندکی هموار کرده و امیدوار باشیم ان شاءالله در آینده‌ی نزدیک توسط سایر پژوهشگران، مسائل این حوزه روشن‌تر شود.

۳.۰ سوالات و فرضیه‌های پژوهش

سوالات اصلی‌ای که در این پژوهش به دنبال پاسخ به آن‌ها هستیم عبارتند از:

۱- سیاست کیفری ایران در قبال جرایم رایانه‌ای چیست؟

۲- سیاست کیفری ایران در قبال هک چیست؟

در پاسخ به سوالات مطرح شده، فعلاً تصور و فرضیه این است که قانون‌گذار به دلایل متعدد، سیاست کیفری ناقص و غیرصحیحی در جرایم رایانه‌ای اتخاذ کرده است، ناقص از این جهت که در خصوص آثار حقوقی بسیاری از فناوری‌های نوین ساکت است، غیرصحیح از این جهت که به دلیل عدم آشنایی دقیق با مباحث فنی این حوزه، صرفاً با چسباندن صفت رایانه‌ای به جرایم سنتی و تشدید کردن مجازات، تکلیف را از خود ساقط کرده است، همچنین در چند مورد جرم خاص رایانه‌ای هم عجزولانه بدون در نظر گرفتن فعل مادی‌ای که توسط هکر انجام می‌شود جرم انگاری عجزولانه‌ای صورت گرفته است.

بنابراین ما در این پژوهش به دنبال کشف سیاست کیفری نیستیم (چون تقریباً سیاست مشخصی وجود ندارد)، بلکه سعی داریم سیاست کیفری مناسب جمهوری اسلامی را در جرایم رایانه‌ای و به طور ویژه در هک تبیین کنیم.

۴.۰ شیوه انجام پژوهش

در فصل اول با مراجعه به منابع و مستندات معتبر و اسناد به داده‌های کتابخانه‌ای، مبانی، مفاهیم و پیشینه‌ی هک گردآوری می‌شود.

در فصل دوم و سوم با مراجعه به مستندات فنی هک و امنیت، و با مشاهده و تجربه‌ی آنچه در عمل توسط هکر اتفاق می‌افتد، ابتدا فعل مادی هر مرحله‌ی هک توصیف، سپس با جرایم رایانه‌ای مندرج در قوانین تطبیق زده می‌شود تا خला‌های قانونی کشف شود؛ همچنین عنداللزوم با مصاحبه و استخراج داده‌ها از پلیس فتا و دادسرای جرایم رایانه‌ای در هر جرم، سیاست کیفری قضایی توصیف می‌شود. در انتها با توجه به فصول گذشته، سعی می‌شود خارج از چهارچوب قانون جرایم رایانه‌ای، ساختار مناسب در خصوص سیاست کیفری مناسب برای جرایم این حوزه پیشنهاد و تشریح شود.

۵.۰ پیشینه پژوهش

در موضوع جرایم رایانه‌ای کتب، پایان‌نامه‌ها و مقالات متعددی نوشته شده است که هر یک به زعم خود نقشی در افزایش دانش فارسی در این زمینه داشته‌اند و ما هم در این پژوهش به دفعات از این منابع استفاده کرده و به آنها اسناد می‌دهیم، که در ادامه سعی می‌شود به طور خلاصه به بعضی از آنها اشاره شود.

۱.۵.۰ کتاب جرایم رایانه‌ای

اولریش زیبر حقوقدان برجسته آلمانی در کتاب جرایم رایانه‌ای که توسط محمدعلی نوری و همکاران ترجمه شده است به بررسی موضوعاتی از جمله مقدمه و ظهور خطر جدید، تعریف جرم رایانه‌ای، محدوده اثرات جرم رایانه‌ای و تحولات آن در آینده، مسائل حقوقی مربوط به جرم رایانه‌ای، تعقیب جرم رایانه‌ای و ... پرداخته‌است.

۲.۵.۰ کتاب درآمدی بر آیین دادرسی کیفری جرایم سایبری

امیرحسین جلالی فراهانی در این کتاب به بررسی صلاحیت کیفری در فضای سایبر، استنادپذیری ادله الکترونیکی، صلاحیت کیفری در فضای سایبر، صلاحیت سرزمینی و ... پرداخته‌است.

۳.۵.۰ کتاب پی‌جویی جرایم رایانه‌ای

رضا پرویزی در این کتاب به مباحثی از جمله تعریف و سابقه جرم رایانه‌ای، نقش پلیس در مبارزه با جرایم رایانه‌ای، بررسی صحنه‌ی جرم رایانه‌ای و ... پرداخته‌است.