بسم الله الرحمن الرحیم

دانشکده معارف اسلامی و حقوق

پایان‌نامه 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

خداوند متعال را بابت اعطای فرصت کسب‌علم 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 داده‌نشود ممکن است باعث خسارات بسیار بزرگ به دولت و جامعه شود، مسائلی مانند هوش‌مصنوعی، 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 اولا ضعف‌های قوانین فعلی آشکار شود، ثانیا فضای جرایم سایبری و ابعاد فنی آن برای حقوق‌دانان واضح‌تر شود و ثالثا راهکارهایی برای سیاست‌گذاری و قانون‌گذاری در این حوزه ارائه شود.

کلمات کلیدی: جرم رایانه‌ای، سیاست کیفری، هک

فهرست مطالب

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 اکثرا با سیستم‌های آنلاین و از راه دور کنترل می‌شوند، به زودی منازل مسکونی، فروشگاه‌ها و ... مجهز به اینترنت اشیاء[1] شده و از راه دور کنترل می‌شوند، این تحولات قطعا اقتضائات خاص خود را هم به همراه دارد.

نظام‌های حقوقی همواره در جریان تحولات فعال بوده و پاسخ‌هایی را به مسائل مستحدثه داده است، طبعا 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 طبیعتا وقتی بسترهای ارتکاب جرم تغییر کند مجرمین هم تغییر می‌کنند، مجرمین دیگر افرادی پرزور نیستند که نهایتا 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

[1] internet of things(IOT)

دولت به معنای عام برای مدیریت جرم اتخاذ می‌شود، مشتمل بر جرم‌انگاری، مسئولیت کیفری و شدت کیفردهی. (مهرا، ۱۳۹۷: ۵۳-٦٦)

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 جرم‌انگاریِ 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 ۱۳۹٤ 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 تحول های بسیار بزرگی در زمینه‌های مختلفی شده است، فناوری‌هایی مانند زنجیره بلوکی[۲]، گسترش شبکه وب تاریک[۳]، گسترش پردازش ابری[٤]، روش‌های جدید رمزنگاری[٥]، گسترش اینترنت اشیاء، رمزارزها[٦]، داده‌کاوی[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 رایانه ای، اقدام به جرم‌انگاری کرده است، رویکرد فعلی

[2] blockchain
[3] Dark Web
[4] cloud computing
[5] cryptography
[6] cryptocurrency
[7] data mining
[8] artificial intelligence
[9] machine learning
[10] deep learning

نسبت به جرایم رایانه‌ای مانند این است که قانون‌گذار در جرم قتل عمد با چاقو این‌گونه جرم‌انگاری کند: تهیه چاقو یک‌سال حبس، پیداکردن محل زندگی مجنی علیه یک‌سال حبس، زیرنظرگرفتن بزه‌دیده یک‌سال حبس، ورود به منزل بزه‌دیده یک‌سال حبس، داخل‌کردن چاقو در بدن یک‌سال حبس، ازهاق نفس پنج سال حبس، ریختن خون روی زمین هم یک‌سال حبس! در خصوص جرایم سایبری الان دقیقا اینگونه رفتار شده است؛ هکر در یک فرآیند هک، مجموعه اقداماتی را انجام می‌دهد تا به هدف خود برسد، قانون گذار 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 واسط‌ها، 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 تشدیدی است، منتهی در خصوص هک هیچ رویکرد شفاف و یکپارچه ای نداریم و بعضا میتوان از بررسی جرایم پراکنده‌ی رایانه‌ای مانند شنود رایانه‌ای، دسترسی غیرمجاز و ... حدس هایی 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 همه‌گیرشدن 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 قوه‌ی 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 CEH[11] در تمام مراحل هک بررسی کنیم، هم مصادیقی که هک در آن موضوعیت دارد مانند هک شبکه، سرور، وبسایت‌ها، موبایل، رایانش ابری، اینترنت اشیاء و ... و هم مباحثی که هک به عنوان وسیله استفاده می‌شود مانند تروریسم سایبری[۱۲]، جنگ سایبری[۱۳]، پولشویی از طریق رمزارزها، معاونت در جرائم ارتکابی در بستر دارک‌وب مانند معاونت در قتل، آدم‌ربایی، تجاوز، فروش موادمخدر 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 آینده ی 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، فعلا 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، صرفا 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 عجولانه بدون در نظر گرفتن فعل مادی‌ای که توسط هکر انجام می‌شود جرم انگاری عجولانه ای صورت گرفته است.
بنابراین ما در این پژوهش به دنبال کشف سیاست کیفری نیستیم(چون تقریبا سیاست مشخصی وجود ندارد)، بلکه سعی داریم سیاست کیفری مناسب جمهوری اسلامی را در جرایم رایانه‌ای و به طور ویژه در هک تبیین کنیم.

٤.۰ شیوه انجام پژوهش

در فصل اول با مراجعه به منابع و مستندات معتبر و اسناد به داده‌های کتابخانه ای، 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 خلاهای 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.