دانشگاه تهران

دانشکده حقوق و علوم سیاسی

پایان نامه برای اخذ درجه کارشناسی ارشد در رشته حقوق جزا و جرم شناسی

جرایم علیه تمامیت داده ها و سامانه های رایانه ای

استاد راهنما: آقای دکتر محسن رهامی

استاد مشاور: آقای دکتر محسن صادقی

دانشجو: نیما نادرخانی

تابستان 1390

به نام یگانه هستی بخش

نفس می نیارم زد از شکر دوست که شکری ندانم که درخورد اوست

عطاییست هر موی ازو بر تنم چگونه بهر موی شکری کنم ؟

ستایش خداوند بخشنده را که موجود کرد از عدم بنده را

(سعدی شیرازی)

تقدیم به آنان که جز در راه حق، گام بر نمی دارند

چکیده

حفاظت از تمامیت عناصر رایانه ای، یکی از اهداف اساسی در وضع قوانین مربوط به جرایم رایانه ای در هر کشوری است؛ این ارزش هم پایه و یا حتی بیش از سایر ارزشهای موجود در عرصه الکترونیکی، مورد حمایت قرار گرفته است، چرا که یکی از ابتدایی ترین و با اهمیت ترین حقوق در این عرصه، در امان بودن اشخاص از تعرض به تمامیت داده ها و سامانه های رایانه ای آنهاست. جرایمی که بر ضد تمامیت در فضای الکترونیکی قابل وقوع هستند و در قانون جرایم رایانه ای ایران از آنها به عنوان دو جرم علیه تمامیت داده ها و سامانه های رایانه ای نام برده شده است، مشتمل بر دو جرم اصلی می باشند؛ یکی از این دو، جرم تخریب داده های رایانه ای است، که مرتکب آن درصدد ایراد ضرر و آسیب رسانیدن بدون حق به داده رایانه ای است؛ و دیگری، جرم اخلال در سامانه های رایانه ای است، که مرتکب آن به توسط انجام اقداماتی بدون حق بر روی داده های رایانه ای، می خواهد به سامانه رایانه ای آسیب برساند و یا کارکرد آن را مختل سازد. هر دوی این جرایم را می توان تحت عنوان تخریب رایانه ای بررسی نمود و البته نباید این نکته را از نظر دور داشت که جرایمی چون تروریسم و سابوتاژ رایانه ای نیز علی رغم وجود سبقه ی امنیتی در آنها، ماهیتاً از زمره زیر شاخه های جرایم علیه تمامیت داده ها و سامانه های رایانه ای محسوب می گردند. مع الوصف یافته های این پژوهش حکایت از آن دارند که تخریب رایانه ای ماهیتی بسیار متمایز از جرایم سنتی دارد، این تفاوت بویژه زمانی آشکارتر می گردد که ارکان اختصاصی متشکله این جرم را جزء به جزء بررسی و با جرم تخریب سنتی مقایسه نماییم. لذا خاص بودن ارکان مادی و معنوی جرایم علیه تمامیت داده ها و سامانه های رایانه ای خود نشان از منحصر به فرد بودن این نوع از جرایم دارد. آشنایی با مفاهیم اساسی هر یک از این جرایم و بررسی ارکان سه گانه آنها، هدف این پژوهش است که در این راستا به کار گیری اسناد بین المللی چون کنوانسیون جرایم سایبر و توصیه نامه شورای اروپا می تواند در تطبیق با قانون جرایم رایانه ای یاری رسان ما در انجام این مهم باشد.

واژگان کلیدی: جرم رایانه ای، جرم سایبر، تمامیت داده، تخریب اموال، تخریب داده، اخلال در سامانه، داده، سامانه رایانه ای.

فهرست

مقدمه 1

1- طرح موضوع 2

2- انگیزه انتخاب موضوع و ضرورت انجام پژوهش 8

3- اهداف پژوهش 10

4- پرسش و فرضیه 11

5- روش و دشواری های پژوهش 12

6- پیشینه پژوهش 13

7- ساماندهی پژوهش 14

فصل نخست. تخریب داده های رایانه ای.....16

مبحث نخست. شناخت جرم تخریب داده های رایانه ای 21

گفتار نخست. مفهوم شناسی 21

بند نخست. مفهوم تخریب 21

بند دوم. داده های رایانه ای 23

الف. مفهوم داده های رایانه ای 24

ب. تبیین ماهیت داده های رایانه ای و علت حمایت از آنها 28

گفتار دوم. پدیده شناسی جرم تخریب داده های رایانه ای 35

مبحث دوم. بررسی ارکان جرم تخریب داده های رایانه ای 39

گفتار نخست. رکن قانونی 39

گفتار دوم. رکن مادی 43

بند نخست. رفتار مجرمانه جرم تخریب داده های رایانه ای 44

الف. مصادیق رفتار مجرمانه 49

یک. حذف کردن 49

دو. تخریب کردن 51

سه. مختل کردن 53
چهار. غیر قابل پردازش کردن 53
ب. شیوه و وسیله ارتکاب جرم 54
یک.شیوه ارتکاب جرم 55
دو.وسیله ارتکاب جرم 63
پ. وصف مرتکب 64
بند دوم. شرایط و اوضاع و احوال لازم برای تحقق جرم تخریب داده های رایانه ای 67
الف. موضوع، داده های رایانه ای باشد 67
ب. داده رایانه ای برای دیگری باشد 69
پ. عملیات مرتکب غیر مجاز باشد 75
بند سوم. نتیجه جرم 77
گفتار سوم ـ رکن معنوی 82
بند نخست. علم مرتکب 83
بند دوم. سوء نیت عام 84
بند سوم. سوء نیت خاص 87
بند چهارم. انگیزه 89
مبحث سوم. مجازات جرم تخریب داده های رایانه ای 91
مبحث چهارم. بررسی ماده 131 قانون مجازات جرایم نیروهای مسلح 94
فصل سوم. اخلال در سامانه های رایانه ای 98
مبحث نخست. شناخت اخلال در سامانه های رایانه ای 102
گفتار نخست. مفهوم شناسی 102
بند نخست. مفهوم اخلال 102
بند دوم. مفهوم سامانه 104
گفتار دوم. پدیده شناسی جرم اخلال در سامانه های رایانه ای 106
مبحث دوم. بررسی ارکان جرم اخلال در سامانه های رایانه ای 108
گفتار نخست. رکن قانونی 109
گفتار دوم. رکن مادی 111

بند نخست. رفتار مجرمانه جرم اخلال در سامانه های رایانه ای 111
الف. مصادیق رفتار مجرمانه 114
یک. وارد کردن 116
دو. انتقال دادن 118
سه. پخش کردن 119
چهار. متوقف کردن.....119
پنج. دستکاری.....121
شش. حذف و تخریب کردن.....121
ب. شیوه و وسیله ارتکاب جرم 121
یک. شیوه ارتکاب جرم 55
دو. وسیله ارتکاب جرم 63
بند دوم. شرایط و اوضاع و احوال لازم برای تحقق جرم اخلال در سامانه های رایانه ای 127
الف. موضوع، سامانه رایانه ای باشد 128
ب- سامانه رایانه ای برای دیگری باشد 130
پ. عملیات مرتکب غیر مجاز باشد 133
ت. افعال مجرمانه بر روی داده ها یا امواج الکترو مغناطیسی یا نوری انجام شده باشد 133
بند سوم. نتیجه جرم 135
الف. لزوم تحقق نتیجه مجرمانه 136
ب. ضرر و رکن ضرری 138
پ. شروع به جرم 145
گفتار سوم ـ رکن معنوی 147
بند نخست.علم مرتکب 147
بند دوم. سوء نیت عام.....148
بند سوم. سوء نیت خاص 149
بند چهارم. انگیزه 152

مبحث سوم. مجازات 153

مبحث چهارم. جرایم یا اعمال مرتبط با جرم اخلال در سامانه های رایانه ای 159

گفتار نخست. جرایم امنیتی 159

بند نخست. سابوتاژ رایانه ای 160

بند دوم. تروریسم رایانه ای 171

گفتار دوم. جرایم غیر امنیتی 180

بند نخست. جرم ممانعت از دستیابی به داده ها یا سامانه های رایانه ای 181

بند دوم. ارسال تبلیغات ناخواسته به نشانی پست الکترونیکی دیگران 186

نتیجه گیری و پیشنهاد ها 189

فهرست منابع 199

مقدمه

هزاران سال پیش، زمانی که بشر پا به عرصه وجود نهاد، خانه اش در غار بود و تنها دغدغه اش شکار، پوشاکی جز برگ درختان برایش نبود و ابزاری جز سنگ اورا یاری نمی رساند؛ اما این مخلوق شگفت انگیز خدا نعمتی در سر داشت که سایر مخلوقات را از آن بهره ای نبود. پرسشی را همواره در سر می پروراندم به راستی چطور بشر این چنینی بدین جا رسید؟

پرسشی به ظاهر ساده، اما به غایت ژرف و معنادار که پاسخ به آن نیازمند مرور هزاران سال زندگی بشر و تلاشهای او برای پیشرفت است. به راستی آیا بشر همواره، همانند قرن معاصر، با همین سرعت رو به جلو می تاخته است یا ما در عصری پویا زندگی می کنیم؟ صاحب نظران علوم، همواره از اختراعاتی همچون ماشین بخار یا دستگاه چاپ به عنوان سر آغاز بسیاری از پیشرفتهای بشری یاد می کنند. اما آنچه که مسلم است، سرعت جلو رفت امروزی دنیا، تنها مرهون یک چیز است وآن هم دانش رایانه.

بشر غارنشین آنچنان مأنوس با این طوفان شده است، که زیستن برای او بدون آن امری است قطعاً ناممکن؛ ولیکن بشر تنها در نیکو پنداران خلاصه نمی شود، بلکه در این میان هستند انسانهایی بدسرشت که از این چاقوی نوین برای پیشبرد مقاصد شوم خود استفاده خواهند نمود و رایانه را به مثابه سلاحی مخرب به کار خواهند بست؛ سلاحی که در ظاهر شاید به اندازه کلت و ژسه دهشت آور به نظر نیاید، اما در عالم واقع بیش از آنها می تواند مخرب و ویرانگر باشد. پس ابتذال و مفسده ای که سوء استفاده از رایانه می تواند به همراه داشته باشد به مراتب سهمگین تر از گذشته شده است؛ آری، آنجا جاییست که همه امکان ملاقات یا ارتباط با یکدیگر را دارند، اما آیا در گذشته چنین جایی می شناختید؟

اینها همه و همه شواهد و دلایلی است بر اینکه، عزم خود را بیش از پیش جزم کنیم تا لااقل در جامعه مجازی رایانه ای، جامعه ای آرمانی داشته باشیم، کاری که هیچ وقت در جامعه واقعی از پس آن برنیامدیم!

ساخت مدینه فاضله مجازی نیاز به ابزار دارد، وضع یک قانون کارآمد نخستین حربه در این راستا تلقی می گردد، اما مهمتر از آن، تزریق فرهنگ سالم است، فرهنگی که خود قانون می تواند در بستر سازی آن کمک نماید تا بدین سان مردم جامعه را با آن مانوس سازد؛ البته مسلماً فرهنگ سازی در این زمینه آن هم در بین انسان هایی که اکثر آنها به وجود اجتماع های مجازی و رعایت ضوابط آن بی اعتقادند، کاری است بس دشوار.

یکی از راهکارهای مناسب در فرهنگ سازی و مقابله با ضد ارزش های جامعه مجازی مطالعه و پژوهش در زمینه رایانه و ضد هنجارهایی است که آن را مورد تهدید قرار می دهند؛ پس شایسته است هر کس به اندازه توان خود در این مسیر مقدس گام بردارد و به نوبه خود برای چالش های پیش رو چاره ای بیندیشد که اگر غیر از این باشد، دنیایی جنگل گونه خواهیم داشت؛ همچنانکه بزرگی می گوید:

«دنیا جای خطرناکی برای زندگی است؛ نه به خاطر مردمان شرور، بلکه به خاطرکسانی که شرارتها را می بینند و کاری در مورد آن ها انجام نمی دهند.» (آلبرت انیشتین)

در ادامه در قالب مقدمه، به تبیین اجزا و ارکان اساسی آن که متشکل از شناخت موضوع، ضرورت انجام پژوهش، اهداف، پیشینه، پرسشها و فرضیات، گستره، روش و ساماندهی پژوهش می باشد، خواهیم پرداخت.

1- طرح موضوع

برای دست یازیدن به شناختی مناسب از جرایم علیه تمامیت داده ها و سامانه های رایانه ای و به طور کلی هر جرم رایانه ای دیگری، ابتدائاً نیازمند شناخت ارزش هایی هستیم که در فضای سایبر[1] و

1. Cyber Space

اصطلاح «سایبر اسپیس» اولین بار توسط ویلیام گیبسون(William Ford Gibson) در کتاب تخیلی «ساحر» در سال 1984 مورد استفاده قرار گرفت. (معظمی فراهانی،1383:31)

[«سایبر اسپیس»]محیطی است مجازی و غیر ملموس موجود در فضای شبکه های بین المللی(این شبکه ها از طریق شاهراه اطلاعاتی مثل اینترنت بهم وصل هستند) که در این محیط تمام اطلاعات راجع به روابط افراد، فرهنگها، ملت ها، کشورها و بطور کلی هر

رایانه محترم بوده و تحت حمایت می باشند؛ بنابراین هرگاه به ارزشی از ارزشهای موجود در فضای سایبر و رایانه -که محترم بوده و تحت حمایت می باشند- تعرضی صورت بگیرد، محتملاً جرمی رایانه ای واقع شده است. هر جامعه ای در درون خود دارای اصول و ارزش هایی است که افراد آن جامعه موظف به رعایت آن هنجارها و ارزشها هستند، فلذا اگر فردی از این ارزشها تخطی کند، جامعه به آن فرد به چشم یک فرد نابهنجار و کجرو نگاه می نماید، که در بد ترین و شدیدترین حالت، ضمانت اجرای عدم احترام به ارزشهای جامعه، مجازات فرد متخلف یا مجرم است.

فضای سایبر به دلیل ویژگیهای منحصر به فرد خود، بالاخص خصایص ارتباطی که دارد، امروزه به مثابه یک جامعه گسترده مطرح است؛ جامعه ای مجازی که ابعادی بین المللی دارد و اهمیت آن فراتر از تمامی جوامعی است که بشر تا کنون به چشم خود دیده است.

از جمله اصول حاکم بر فناوری اطلاعات و امنیت رایانه، اصل جریان آزاد اطلاعات است؛[2] که رعایت این اصل در پرتو احترام و حمایت از محرمانگی، تمامیت و دسترس پذیری داده ها و اطلاعات میسر خواهد بود و بنابر این اصل داده ها و اطلاعات در فضای سایبر ساری و جاری هستند و باید

آنچه در کره ی خاکی به صورت فیزیکی و ملموس وجود دارد (به صورت نوشته، تصویر، صوت و اسناد) در یک فضای مجازی به شکل دیجیتال وجود داشته و قابل استفاده و دسترس استفاده کنندگان و کاربران می باشند و به طریق کامپیوتر اجزاء آن شبکه های بین المللی بهم مرتبط می باشد. (پرویزی،48:1384)و (خرم آبادی، 56:1384)

برخی در جهت معادل سازی واژه «سایبر» در زبان پارسی،واژه «مجازی» را پیشنهاد می نمایند، لیکن «به توصیه متخصصان و دانشمندان صاحب نام این رشته، یافتن لغت معادل و یا ترجمه واژه سایبر به زبان های دیگر مجاز نمی‌باشد، چراکه به عقیده این صاحب نظران بسط مفهوم لغوی این واژه در سطح بین‌المللی آن را تبدیل به یک لغت بین‌المللی نموده و ترجمه آن ممکن است باعث محدود شدن معنای آن و عدم ارائه مفهوم صحیح گردد.» (پرویزی،46:1384)

2 - این اصل مهم و اساسی آن دسته از کشورهای دنیا را که داعیه رعایت دموکراسی دارند، بر آن داشته است که به وضع قوانینی در حمایت از این اصل با اهمیت مبادرت نمایند. در فضای سایبر, اطلاعات باید جریان یابد، پس جریان اطلاعات باید قانونمند باشد؛ با یک بررسی تاریخی در خصوص سابقه جریان آزاد اطلاعات متوجه می‌شویم که نخستین تجربه مشخص قانون‌گذاری در زمینه آزادی اطلاعات، به کشور سوئد و سال 1776م برمی‌گردد. هدف از تصویب این قانون که در ابتدا قانون آزادی مطبوعات نام داشت، ایجاد یک جامعه باز بود که در آن حتی اسنادی چون نامه‌های رؤسای کشورهای دیگر به نخست‌وزیر نیز باید تحت نظارت عموم قرار بگیرد؛ قاعده‌ای که تا امروز نیز پابرجا است. کلمبیا پس از سوئد دومین کشوری است که قانون آزادی اطلاعات در آن به تصویب رسیده است. قانون آزادی اطلاعات این کشور (مصوب 1888 میلادی)، دسترسی به اطلاعات و اسناد و مدارک دولتی را حق مردم می‌دانست. بر اساس این قانون، هر فردی می توانست با دادن تقاضا به اسناد دولتی دسترسی داشته باشد، مگر در مواقعی که قانون این دسترسی را محدود کرده باشد. قانون اساسی کنونی کلمبیا نیز همچنان حق دسترسی به اطلاعات در اختیار دولت را تضمین کرده است. فنلاند نیز، سومین کشوری است که قانون آزادی اطلاعات آن در سال 1919م به تصویب رسید.»

(بلخ ژورنالیسم،1389: http://www.balkhjournalism.blogsky.com/1388/07/26/post-696)

آزادی این جریان تحت حمایت قرار گیرد، لذا هیچ کس نمی تواند بدون اینکه حقی داشته باشد، اقدام به ایجاد محدودیت یا خلل در جریان آزادانه اطلاعات نماید. البته این آزادی بی حد و مرز نیست، بلکه در مسائل امنیتی، موارد حریم خصوصی افراد، اسرار دولتی مهم و مسائل بهداشتی این آزادی نفی می شود. تمامی آنچه که به عنوان ارزش های مورد حمایت در فضای سایبر در این بخش بدانها اشاره می گردد، از این حیث حایز اهمیت می باشند که هر کجا بدانها تعرضی صورت گیرد، غالباً نظام حقوقی و تقنینی کشورها با آن پدیده های معارض مبارزه می نمایند؛ به دیگر سخن سنجه جرم انگاری در فضای رایانه ای و سایبری، خلل وارد آوردن به همین ارزشهاست.

در ادامه، به تبیین مختصر این ارزشها که ارکان اساسی یک جامعه مجازی[3] محسوب می گردند، می پردازیم:

یک. محرمانگی[4] داده‌ها و اطلاعات

این عامل باعث می‌شود تا کسانی که هیچ گونه مجوزی ندارند یا اجازه آنها به اندازه ای نیست که بتوانند از آن اطلاعات استفاده کنند از دسترسی به آن اطلاعات منع شوند، در حقیقت تعرض به این عامل، تجاوز به حقوق مشروع دیگران مبنی بر حفظ اطلاعات شخصی و خصوصی آنها می‌باشد. تعرض به این عامل عمدتاً زمانی به وقوع می‌پیوندد که یک متعرض (هکر) اطلاعات کاربر یا آنچه که متعلق به او می‌باشد را، بدون اجازه، مشاهده یا کپی نماید.

دو. دسترس پذیری[5] اطلاعات و خدمات

حفظ عملکرد مفید سیستم و در دسترس نگهداشتن آن برای جامعه و افراد ایجاد که نیازمند حمایت جدی می‌باشند در پرتو دسترس پذیر ماندن اطلاعات تحقق می یابد. که بیانگر این مطلب است که تحصیل اطلاعات و برنامه‌های مرتبط با آن از طرف یک کاربر، آن هم زمانی که بدان احتیاج دارد، نشانگر مفید و کاربردی بودن آنهاست.

3 - Virtual Society.
4 - Confidentiality
5 - Availability

نقض این عامل زمانی به وقوع می‌پیوندد که کاربر دارای مجوز برای مدتی از ارتباط مستمر و قابل اتکا و اطمینان با سیستم و مرکز مورد نظر خود باز می‌ماند و از آن منع می‌شود. نمونه بارز و معمولی که در این رابطه به وقوع می‌پیوندد حملات داس[6] می‌باشد، که از فعالیت عضو انجمن سیستمهای اطلاعاتی «اِی آی اِس»[7] مطابق با اهدافی که برای آن پیش‌بینی شده جلوگیری می کند. این عمل ممکن است شامل جلوگیری از ارائه سرویس با فرآیندهای محدود شده‌ای به سیستم میزبان شود، با این حال این اصطلاح اغلب دلالت بر فعالیتهای علیه یک میزبان یا یک گروه از آنها دارد که باعث غیرفعال شدن آنها در زمینه ارائه خدمات به کاربران خصوصاً در ارتباط با شبکه می باشد.

سه. تمامیت[8] داده‌ها و اطلاعات

تمامیت اطلاعات در معنای خاص خود به معنی حفظ اصالت و هست مندی، در برابر تحریفات یا آسیب به آنهاست، اما این اصطلاح در معنای عام خود شامل صحت اطلاعات و داده ها نیز می باشد و این اطمینان را به وجود می آورد که هیچ کس نمی تواند بدون داشتن حق، اطلاعات مورد احتیاج دیگری را تغییر داده یا تخریب نماید؛ لذا هرگونه اضرار یا تحریف اطلاعات یا داده های رایانه ای، که بدون حق صورت گیرد، با تمامیت اطلاعات و در نتیجه با جریان آزاد اطلاعات مغایرت دارد. و این اطمینان را به وجود می آورد که هیچ کس نمی تواند بدون داشتن حق، اطلاعات مورد احتیاج دیگری را تغییر داده یا تخریب نماید؛ لذا هرگونه اضرار یا تحریف اطلاعات یا داده های رایانه ای، که بدون حق صورت گیرد، با تمامیت اطلاعات و در نتیجه با جریان آزاد اطلاعات مغایرت دارد.

تمامیت داده ها را به شرح زیر تعریف نموده است:

«نمادی است اختصاصی از صحت و کمال موجودیت داده ها و اطلاعات و همچنین حفظ این صحت و موجودیت داده ها.»[9] (OECD, 1992, OECD Guidelines for the Security of Information Systems)

---

6 -Denial Of Service attack (DOS).

7- Associations Information System (AIS).

8 - Integrity

9- در خصوص مفهوم تمامیت داده یا اطلاعات متن قانونی خاصی در دسترس نسیت، لیکن بند «ه» از ماده 2 قانون تجارت الکترونیکی تنها قانون داخلی است که به نوعی تلویحاً توجه خود را به تمامیت داده معطوف ساخته است، البته هرچند که در آن از اصطلاح

در ادامه، لازم به یادآوری است که بنا بر یک تعبیر، اصل تمامیت داده ها و سامانه‌ها، اصل عام الشمولی است که در معنای کلی خود، حتی اصل دسترس‌پذیری را در بر می‌گیرد؛ همچنین در باب تفاوت محرمانگی داده ها با تمامیت داده ها باید این نکته را در نظر داشت که ارزش صحت و تمامیت برای خود داده و سامانه است، ولی ارزش محرمانگی برای دارنده آنها.

در کنوانسیون جرایم سایبر جرایم برضد محرمانگی، تمامیت در دسترس بودن داده‌ها و سامانه‌های رایانه‌ای تحت یک طبقه و با هم آمده‌اند و بر این اساس، جرایمی که در این دسته قرار میگیرند، عبارتند از: دستیابی عمومی و من غیرحق به سامانه‌های رایانه‌ای، شنود عمدی و من غیرحق به سامانه-های رایانه‌ای، ایجاد اختلال عمد و من غیرحق در داده‌های رایانه‌ای،ایجاد اختلال عمدی و من غیرحق در سامانه‌های رایانه‌ای، سوءاستفاده از وسایل رمز عبور و کد دستیابی یا داده‌ها یا برنامه‌های رایانه‌ای؛ همان طور که ملاحظه می شود کنوانسیون مزبور کلیه جرایمی را که تهدیدی علیه اصل جریان آزاد اطلاعات تلقی می گردند، در یک دسته قرار داده است.

در میان ارزش هایی که از آنها یاد کردیم، سومین مورد -که به نظر نگارنده مهم ترین آنها نیز به حساب می آید- شالوده شکل گیری پژوهش پیش رو را تشکیل داده است. تعرض به این ارزش -که به شکل یک اصل در حقوق فناوری اطلاعات نیز در آمده است- منجر به تحقق جرایمی چون تخریب داده ها یا اخلال در سامانه های رایانه ای می گردد، که در نهایت نیز می تواند منتج به تحقق جرایم مشابه سنگین تری مثل خرابکاری و تروریسم رایانه ای گردد.[10]

تمامیت داده پیام استفاده شده است اما از آنجا که داده پیام ها نیز خود نوعی از داده ها تلقی میشوند، لذا تعبیر مقرره مزبور از «تمامیت داده پیام» میتواند برای ما مفید فایده واقع شود. این مقرره قانونی اشعار می دارد : «تمامیت داده‌پیام عبارت است از موجودیت کامل و بدون تغییر داده‌پیام.» همچنین در ادامه این ماده آمده است: «اعمال ناشی از تصدی سیستم از قبیل ارسال، ذخیره یا نمایش اطلاعات که به طور معمول انجام می شود خدشه‌ای به تمامیت «داده‌پیام» وارد نمی‌کند.» از متن مقرره فوق می توان برداشت نمود که، تمامیت داده ها به موجودیت، اصالت یا همان هست مندی آنها برمی گردد.

10 - در این زمینه گفته اند: «بسیاری از تعرضات عمدی که توسط هکرها صورت می‌گیرد، مانند وارد کردن ویروس های رایانه‌ای از قبیل کِرم‌ها و اسب های تروا در این رده جای می‌گیرند. این امر نه تنها از جانب کسانی که منافع اقتصادی را دنبال می‌کنند به وقوع می‌پیوندد، بلکه آنهایی که قصد مقابله به مثل (انتقام)، اعتراض سیاسی، تروریسم یا صرفاً قصد رقابت داشته باشند نیز مرتکب آن می‌شوند.» (خرم آبادی،1384 :19)

صحت داده ها نیز از جمله اصطلاحاتی که غالباً در کنار و همراه تمامیت داده می آید، آن هم به دلیل ارتباط معنایی است که بین این دو وجود دارد، ولیکن صحت داده ها را باید ارزشی خاص و متفاوت از تمامیت اطلاعات محسوب داشت. در این خصوص یکی از نویسندگان می نویسد:«صحت به معنای اصالت و داشتن هویت راستین است؛ صحت ویژگی داده و سامانه ای است که بتوان بر پایه آن، هم از جهت ظاهری و هم از جهت معنایی به درست بودن آن بی گمان بود. تمامیت به هستی و یکپارچگی داده و سامانه نگاه دارد. با این حال این دو واژه یکی نیستند واصل صحت برای پشتیبانی از ناب‌مندی (اصالت و قابلیت استناد) است ولی تمامیت برای هست‌مندی (موجودیت) و نیز صحت بیشتر ویژگی داده است ولی تمامیت هم بر داده روی می کند و هم بر سامانه. پس جعل رایانه ای صحت داده را تهدید می کند و تخریب و اخلال بر ضد تمامیت داده یا سامانه اند.»[11]

به هر حال اصطلاح تمامیت داده در معنای عام خود می تواند صحت داده را نیز در برگیرد، لیکن مقصود ما از تمامیت داده در این پژوهش معنای خاص آن است که به کلیت و موجودیت داده برمی گردد، نه صحت یا قابلیت استناد آن؛ لذا باور نگارنده بر این است که صحت داده ها خود ارزشی مجزا در فضای سایبر و رایانه به حساب می آید و در عین حال می توان آن را در قالب تمامیت اطلاعات در معنای عام آن نیز قرار داد و بنابر این تفکیک این دو اصطلاح از یکدیگر در تحلیل جرایم رایانه ای مرتبط، به کمک ما خواهد آمد؛ لذا در این پژوهش تنها به جرایمی پرداخته شده است که تمامیت داده ها را در معنای خاصش مورد تهدید قرار می دهند و نه صحت داده ها را؛ به همین جهت نیز جرم جعل که جرمی است بر ضد صحت داده ها از گستره این پژوهش خارج شده است، مضاف بر اینکه هیچ ارتباط موضوعی بین جعل و تخریب رایانه ای وجود نداشته است و پرداختن به هر دوی اینها در قالب

11 -«با این حال این جداسازی در ق.ج.ر دیده نمی شود و حتی در کنار سه رفتار پیش گفته یعنی جعل، تخریب و اخلال، سه رفتار بزهکارانه دیگر نیز پیش بینی شده است که عبارتند از استفاده از داده مجعول که پیوند سرراست با صحت داده ندارد و ممانعت از دسترسی به داده که این بزه نیز بر ضد اصل دسترس پذیری داده است. رفتار سوم نیز تروریسم سایبری است که گستره آن نیز همه رفتارهای پیش گفته را در بر می گیرد.»(عالی پور،198:1390)

یک نوشتار، علاوه بر بالا بردن و خارج نمودن حجم پژوهش از حد استاندارد، منجر به به هم ریختگی مطالب نیز می گردید.

2- انگیزه انتخاب موضوع و ضرورت انجام پژوهش

از زمانی که رایانه پا به عرصه هستی گذارده است شاید زمان زیادی سپری نشده باشد، اما دنیای ما آنقدر متأثر از این فناوری بوده است که امروزه تمامی انسانها را با خود مانوس ساخته است. از این رو، علم رایانه را باید فناوری دگرگون کننده نامید؛ شاید پنجاه سال قبل سخن راندن از جرایم علیه تمامیت اطلاعات، امری غیر قابل درک برای آحاد مردم به حساب می آمد اما امروزه این گونه نیست و غالب مردم بر اهمیت جرایمی چون تخریب رایانه ای که تمامیت اطلاعات را مورد مخاطره قرار می دهند واقف می باشند؛ همین موضوع منجر به آن شده است که تحقیقاتی که در گذشته انجام شده است، امروزه دیگر کارآمد نباشد و توان حل چالشهای فناوری الکترونیکی را نداشته باشد؛ لذا اهمیت انجام پژوهش های نوین و مرتبط با رایانه در میان خلأ تحقیقاتی موجود، بیش از پیش نمودار شده است. بالاخص در قرن حاضر که تجارت الکترونیکی رکن اصلی مبادلات مردم به حساب می آید زیرا توانسته اعتماد مردم را به خود جلب نماید و با توجه به منافعی که دارد مردم را مجاب به کنار گذاشتن طرق سنتی تجارت نموده است؛ بنابراین پرواضح است که اختلال در فضاهای الکترونیکی مساوی است با از دست رفتن تدریجی اعتماد مردم به جامعه مجازی.

دیگر تنها مردم در دنیای واقعی با یکدیگر ارتباط ندارند بلکه در فضای سایبر نیز با یکدیگر تعامل دارند[12]، بنابراین پر واضح است علم حقوق باید به وظیفه خود بیش از پیش عمل نموده و همانطور که وظیفه تنظیم روابط بین اشخاص را برعهده داشته است به این مهم در روابط بین افراد در فضای

12- هر آنچه در دنیای واقعی وجود دارد در فضای مجازی نیز می تواند وجود داشته باشد، با این تفاوت که در فضای واقعی حضور اشیاء و سایر موجودات به صورت فیزیکی و ملموس است ولی در فضای مجازی حضور آنها به صورت غیر ملموس و غیر مادی. در واقع در فضای سایبر چیزی جز داده های رایانه ای وجود ندارد. (خرم آبادی، 1384 : 13)

مجازی[13] نیز جامهٔ عمل بپوشاند، لذا حقوق جزا باید دارای آن چنان مقرراتی باشد که اجرای صحیح «جریان آزاد اطلاعات»[14] را تضمین کند، حقوق جزای سنتی فاقد چنین مقرراتی است، به همین علت نیاز به جرم انگاری در این فضای مجازی، در تمام کشورهای دنیا احساس گردید[15]؛ نتایج و آثار مخربی که جرایم رایانه ای به بار می آورند به مراتب بیش از برخی جرایم سنتی است[16]، همین موضوع به یک عامل محرک برای حقوق کیفری کشورها بدل شده است، تا عزم خود را برای مقابله هر چه شدیدتر با این معضل، جزم کنند و به وضع مقررات حمایتی از عرصه رایانه ای برآیند؛ قوانینی که به موضوع جرایم رایانه ای اختصاص دارند از جمله مهمترین قوانین کیفری کشورها به حساب می آید، لذا چه خوب است که تا حد امکان، قوانین رایانه ای کارآمد و کم اشکال تری داشته باشیم، به همین خاطر در این پژوهش سعی در معرفی نارسایی های موجود در قوانین رایانه ای ایران و راهکاری مناسب در اصلاح آنها نموده ایم.

اما انتخاب موضوع با عنوان جرایم علیه تمامیت داده ها و سامانه رایانه ای به دو دلیل عمده و مهم صورت گرفته است :

1) نخستین دلیل این است که تمامیت داده ها و سامانه های رایانه ای به عنوان ارزشی مهم در فضای سایبر و رایانه محسوب می گردد، که تعرض به آن، منجر به شکل گیری جرم با اهمیتی همچون تخریب رایانه ای گردیده است؛ با اهمیت از این جهت که، جرم مزبور می تواند سرآغاز و نقطه شروع بسیاری از جرایم با اهمیت و خطرناک دیگر همچون تروریسم و سابوتاژ رایانه ای باشد؛ فلذا برخورد با آن، در عین حال، برخورد با تروریسم و سابوتاژ رایانه

14- اصل جریان آزاد اطلاعات: به این معنا که «در محیط دیجیتالی و شبکه های رایانه ای» اصل بر آزاد بودن جریان اطلاعات و دسترسی افراد به اطلاعات است. این آزادی بی حد و مرز نیست، بلکه در مسائل امنیتی، موارد حریم خصوصی افراد، اسرار دولتی مهم و مسائل بهداشتی این آزادی نلفی می شود.(حسن بیگی، 1384:179)

15 - حقوق کیفری سنتی اساساً از کالاهایی که کاملاً ملموس تعریف می‌شوند، در برابر تهاجم‌های بشری حمایت می‌کند اما جرایم رایانه‌ای به ارزش‌های ناملموس نوینی تعرض می‌کنند. (زیبر، 1388: 40)

16 - درآمد حاصل از جرایم اینترنتی در دنیا در این سال ها 105 میلیارد دلار بوده که این میزان 5 برابر درآمد حاصل از فروش مواد مخدر است. (پایگاه اطلاع رسانی تخصصی،1390: http://www.ictpress.ir/Default,fa-IR,ICTPress,Content,NewsDetail,Key,9126.aspx)

ای است، چرا که تا مجرمی از مرحله ابتدایی _ یعنی همان ارتکاب جرم تخریب رایانه ای_گذر نکند، موفق به رسیدن به مراحل بالاتر _ که جرمی چون تروریسم رایانه ای از آن جمله است_ نخواهد شد .

2) دومین دلیلی که در انتخاب موضوع، نگارنده را مصمم تر ساخت، برگزیدن عنوان جرایم علیه تمامیت داده ها و سامانه های رایانه ای توسط قانونگذار ایران برای فصل دوم «قانون جرایم رایانه ای»[17] است، این موضوع نشان گر اهمیت تمامیت اطلاعات در فضای رایانه برای مقنن ایران می باشد، که او را بر آن داشته است تا یک فصل از ق.ج.ر را بدان اختصاص دهد.

3- اهداف پژوهش

خواسته یا ناخواسته پدیده ای مخرب به نام تخریب رایانه ای به شکل تهدید آمیزی پا به عرصه وجود گذارده است؛ این مهمان ناخوانده به سرعت در حال تاختن است. مبارزه با پدیده تخریب رایانه ای نیازمند آشنایی با ابعاد و ویژگی های آن است. در وهله نخست باید این جرم را در حقوق جزای اختصاصی بررسی نماییم و مشخص کنیم که در ارکان سازنده آن چه دگرگونی هایی رخ داده است. بدون شک تا زمانی که با این خصایص آشنا نشویم، سخن راندن از مبارزه با این پدیده، به گزاف خواهد بود.

در این پژوهش سعی خواهیم نمود تا خلل های موجود در ق.ج.ر را به عنوان تنها منبع جامع جرایم رایانه ای، مورد نقد قرار داده و در عین حال نگاهی تطبیقی را در مقایسه با کنوانسیون جرایم سایبر ارایه نماییم و با تمسک به این روش پیشنهادهایی را نیز در راستای مرتفع سازی ایرادات ق.ج.ر در زمینه جرایم علیه تمامیت داده ها و سامانه های رایانه ای مطرح خواهیم نمود و امیدواریم که نقطه آغازی برای انجام سایر پژوهش های تحلیلی در خصوص جرایم رایانه ای موجود در ق.ج.ر ایران باشیم.

17 -از این پس به عنوان جایگزین عبارت «قانون جرایم رایانه ای» از علامت اختصاری آن، یعنی «ق.ج.ر» استفاده خواهیم نمود.

علاوه بر تمامی اینها، رسالتی دیگر را نیز دنبال می کنیم و آنهم آشناسازی کاربران و حقوق دانان با جرایم علیه تمامیت داده ها و سامانه های رایانه ای است تا بدین سان کاربران را به تعرضاتی که ممکن است علیه داده ها و سامانه هایشان انجام شود، آشنا نماییم، همچنین به حقوق دانان و محققانی که تا به حال با جرایم رایانه ای و اهمیت آنها آشنا نبوده اند، نشان دهیم که نباید از کنار این جرایم به سادگی گذشت، زیرا اینها جرایمی هستند که ویژگی های خاص و بی بدیلی دارند که ضمناً می توانند آثار منفی فراوانی را به بار آورند.

4- پرسش و فرضیه پژوهش

پرسش آغازین که در ذهن هر پژوهشگری ابتدائاً شکل می گیرد، نقش اصلی را در رهنمون او به سوی نگارش تحقیق، ایفا می نماید. پرسشی که در ذهن بنده ایجاد شد و اساس شکل گیری این پژوهش را تشکیل داد، پرسش زیر است :

آیا رکن مادی و معنوی جرایم علیه تمامیت داده ها و سامانه های رایانه ای که انواع تخریب رایانه ای را در بر میگیرد، کاملاً مشابه یا منطبق بر رکن مادی و معنوی تخریب سنتی است ؟ و آیا اساساً نیازی به وضع مقررات قانونی مختص به جرایم علیه تمامیت داده ها و سامانه های رایانه ای وجود دارد؟

فرضیه پژوهش نیز در راستای پاسخ به پرسش فوق، به شرح زیر قابل طرح است :

رکن مادی و همچنین رکن معنوی جرایمی که در در حیطه جرایم علیه تمامیت داده ها و سامانه های رایانه ای قرار می گیرند در بسیاری از ابعاد خود با جرایم سنتی مشابه، دارای اختلاف و تمایز هستند و به همین دلیل وجود مقرراتی مخصوص جرایم مزبور لازم و حیاتی است و قوانین کیفری سنتی نمی توانند تمامی وجوه جرایم فوق را در بر گیرند.

5- روش و دشواری های پژوهش

موضوع این پژوهش، موضوعی است مرتبط با حقوق کیفری اختصاصی، بر همین پایه روش اتخاذی اصولاً باید توصیفی باشد. به این صورت که به روشی قیاسی و تمثیلی و با تمسک به ابزار کتابخانه ای، به بررسی نظرات و آثار گذشتگان پرداخته شده و صحت و اعتبار نظریات مذکور مورد تحلیل قرار گیرد. لیکن در این نوشتار اندکی از روش اشاره شده فاصله گرفته ایم؛ زیرا در ایران، تعداد پژوهشهای معتبر صورت گرفته در خصوص جرایم رایانه ای حتی از تعداد انگشتان دست نیز کمتر است، مضاف بر اینکه حتی یک پژوهش مفصل و جامع در زمینه موضوع پایان نامه پیش رو وجود ندارد، علت این موضوع نیز این است که، در پژوهش های حقوق کیفری اختصاصی تحلیل مبتنی بر قانون، اساس پژوهش محسوب خواهد شد، اما از آنجا که ما با قانون نوپای جرایم رایانه ای مواجهیم که از زمان تصویب آن کمتر از دو سال می گذرد، پس بدیهی است که تحقیق های انجام شده در این باره نیز، اندک خواهند بود.

مع الوصف فقدان آراء و نظریات معتبر در این زمینه، خود نشانگر دشواریهای این پژوهش می باشد. نوشتار پیش رو از جمله نخستین پژوهش هایی است که به نحوی تحلیلگرانه به جرم رایانه ای و بالاخص تخریب رایانه ای نگاه داشته است، با وجود این ممکن است کمی و کاستی هایی نیز در خلال این پژوهش به ذهن خواننده برسد که نگارنده منکر آنها نیست، ولیکن ارزش کار خود را بیشتر از آن جهت می داند که شاید تلنگری بر گسترش دامنه پژوهش در زمینه جرایم رایانه ای محسوب گردد. در این راستا برای توصیف شیوا تر مطالب، علاوه بر منابع پارسی از برخی منابع انگلیسی نیز استفاده شده است؛ هر چند که منابع انگلیسی نیز به دلیل کلی بودن نمی توانستند، آن طور که باید، کمکی در پیشبرد بخش تحلیلی پژوهش نمایند.

بر پایه آنچه گفته شد، روش به کاربرده شده در پژوهش پیش رو، از نوع توصیفی- تحلیلی است؛ هرچند بیشتر از آنکه به توصیف وقایع بپردازیم، آنها را به چالش کشیده ایم و حتی می توان ادعا نمود است که هر دو فصل این نوشتار، به طور کامل به روش تحلیلی صورت گرفته است. همچنین در این

نوشتار سعی شده است که تا حد امکان در کنار تحلیلی بودن، تطبیقی بودن مطالب نیز مد نظر قرار گیرد تا پژوهش دچار یک بعدی بودن نشود و در عین حال با نقاط قوت، نارسایی ها و ابهاماتی که در ق.ج.ر ممکن است وجود داشته باشد، آشنا شده و سپس به یک راهکار اصلاحی یا تفسیری مناسب دست یابیم.

6- پیشینه پژوهش

در زمینه جرایم رایانه ای در سطح بین المللی مطالعات گسترده ای صورت گرفته است که به عنوان مثال، تهیه و ارائه کنوانسیون جرایم سایبر توسط شورای اروپا _به عنوان با اهمیت ترین منبع جرایم رایانه ای_ برآیند مطالعات انجام شده در سطح بین المللی است؛ اما همین تحقیقات صورت گرفته نیز بسیار کلی بوده و پدیده ای مثل تخریب رایانه ای[18] مهجور مانده است و تنها به نحوی اجمالی و گذرا بدان پرداخته شده است. در حقوق ایران وضع حتی از این هم بدتر است، چرا که هیچ موضوع نوینی در پژوهشهای مرتبط با جرایم رایانه ای دیده نمی شود و از بدو شروع تحقیق در این زمینه تنها چیزی که مد نظر قرار گرفته است، مطالب عمومی و کلی مربوط به جرایم رایانه ای بوده است، که این نوع تحلیل ها در آثار حقوق دانان جرایم رایانه ای در کشورهای دیگر هم به وفور یافت می شود، فلذا در ایران ابتکاری در این زمینه به خرج داده نشده است.

بنابراین مطالعات موجود در این خصوص در سطح داخلی بسیار محدود و آنهم به شکل کلی بوده است بدون آنکه به طور موردی و تحلیلی به بررسی جرایم مختلف رایانه ای پرداخته شود؛ به دیگر سخن غالب پژوهش های مرتبط با جرایم رایانه ای به توصیف ویژگی ها و مطالب کلی مربوط به

18 - در ادامه پژوهش هر کجا از تخریب رایانه ای سخن به میان آوردیم، مقصودمان جمع دو جرم تخریب داده ها و اخلال در سامانه هاست، و این هم به این دلیل است که هر دوی این عناوین در اصل تخریب رایانه ای محسوب می گردند، با این تفاوت که یکی داده ها را تهدید می کند و دیگری سامانه های رایانه ای را؛ لیکن جمع هر دو عنوان مزبور تحت عنوان تخریب رایانه ای به این جهت صورت گرفته است.