International conference on Recent Research in Science and Technology
Kerman
In cooperation with
Payame Noor university and Farhangian university

Sponsored and Indexed by
CIVILICA
We Respect the Science
The conference is sponsored by CIVILICA, and articles will be indexed in CIVILICA and the National Consortium.

امنیت و حفاظت از حریم خصوصی در رایانش ابری: بحث ها و چالش ها در ایران

احمد فراهی[1]، شهرام دربندی[2] شهروز دربندی[3]

[1] دکترای تخصصی، استادیار پایه 28، مدیر گروه مهندسی کامپیوتر و فناوری اطلاعات دانشگاه پیام نور، afaraahi@pnu.ac
[2] دانشجوی ارشد مهندسی نرم‌افزار دانشگاه پیام نور واحد شهرری، shahramdarbandi79@gmail.com
[3] کارشناسی ارشد حقوق بین الملل دانشگاه آزاد اسلامی واحد تهران غرب، darbandi.shahrooz@wtiau.ac.ir

چکیده

سیستم‌های محاسباتی بطور گسترده‌ای در حال کامل شدن هستند تا بتوانند پاسخگوی نیازهای بشر در مسائل و کاربردهای مختلف علمی، تجاری، اجتماعی و ... باشند. این تکامل در ابعاد مختلفی صورت گرفته است. قدرت و توان محاسباتی و پردازش اطلاعات، ظرفیت ذخیره‌سازی اطلاعات، دردسترس‌پذیری بیشتر منابع و ... از ابعاد مختلف تکامل سیستم‌های محاسباتی محسوب می‌شوند. یارانش ابری یکی از رویکردهای جدید محاسباتی است که در چند سال اخیر مورد توجه بسیار قرار گرفته است و بطور فزاینده‌ای در حال گسترش است. افرادی که در زمینه رایانش ابری فعالیت دارند، به دلیل اینکه از حوزه‌های مختلف IT نظیر نرم‌افزار، پایگاه داده، شبکه و ... وارد آن شده‌اند، دارای دیدگاه‌های مختلفی در مورد آن هستند که همین موضوع سبب ایجاد تعارف و رویکردهای مختلف در مورد رایانش ابری شده است.

در این پژوهش و تحقیق ما سعی کردیم پس از مطالعه گسترده در بین منابع و کتب مختلفی که در زمینه رایاش ابری منتشر شده است، ضمن ارائه انواع مختلف تعاریف و معماری‌هایی که برای یارانش ابری ارائه شده است، شکل صحیح ارتباط بین آنها را بیان کنیم تا ابهاماتی که در این زمینه وجود دارد برای خواننده گرامی رفع گردد. لذا در این پژوهش سعی داریم ضمن برسی و تشریح کامل این فناوری، به برسی دقیق‌تر نکات فنی، خدمات ارائه شده، مشکلات پیش‌رو، مسائل امنیتی و حقوقی آن در ایران بپردازیم.

امید است که با این کار پژوهشی، توانسته باشیم گام مؤثری در معرفی صحیح فناوری رایانش ابری برداشته باشیم و شاهد کاربردهای سازنده آن در ارتقای سطح عملی کشور عزیزمان ایران در هر دو بعد تئوری و عملی باشیم.

کلمات کلیدی

یارانش ابری، سیستم‌های محاسباتی، امنیت حقوقی، حریم خصوصی

1- مقدمه

رایانش ابری صطلاحی است که در سال‌های اول هزاره سوم مطرح شد، اما مفهوم Computing as a Service به خیلی قبل‌تر و حدود دهه شصت میلادی برمیگردد. زمانی که شرکت‌ها می‌توانستند به جای این که خودشان کامپیوتر بخرند، زمانی را برای استفاده از آنها در Mailframeها اجاره کنند. این نوع سرویس‌های TimeSharing با پایین آمدن هزینه تهیه کامپیوترها، از PCها و سپس دیتاسنترهای اشتراکی که شرکت‌ها می‌توانند در آنها داده‌های زیادی ذخیره کنند، عقب ماندند. اما مفهوم دسترسی به قدرت پردازشی، بارها و بارها پس از این زمان، مطرح شده است. در تأمین کنندگان سرویس اپلیکیشن و با ظهور تأمین کنندگان رایانش ابری در مقیاس بزرگ و SaaS ادامه یافت که سرویس‌های وبی آمازون از آن جمله است. (حسین زاده شبستری، 1400)

در واقع، منطق رایانش ابری، اشتراک زمانی یا TimeSharing است. به این معنی که منابع مختلف کامپیوتری میان چند کاربر با استفاده از روش‌های چندبرنامه‌ای و چند وظیفه‌ای به اشتراک گذاشته می‌شود. این راهکار اولین بار در دهه 1950 مورد استفاده قرار گرفت. زمانی که به دلیل قیمت بالا و اندازه بزرگ کامپیوترها، امکان تهیه کامپیوتر برای هر کاربر وجود نداشت، در نتیجه با این روش، چند کاربر به کامپیوتر مرکزی دسترسی داشتند و به طور مشترک از خدمات آن استفاده می‌کردند. بنابراین می‌توان سرویس‌های ابری را تکامل تدریجی راهکارهای به اشتراک‌گذاری کامپیوترها در دهه 1950 دانست. در دهه 1970 میلادی، ایده ماشین‌های مجازی مطرح شد که امکان استفاده از چند محیط محاسباتی متفاوت روی یک محیط فیزیکی واحد را امکان‌پذیر می‌کرد، این ایده، اشتراک زمانی را که در دهه 1950 مطرح شده بود، به سطح جدیدی ارتقا داد. در دهه 1990 میلادی، شرکت‌های مخابراتی امکان دسترسی به ارتباطات مجازی‌سازی شده را ممکن کردند. به این وسیله به جای ایجاد ساختارهای فیزیکی مستقل برای هر کاربر، امکان به اشتراک‌گذاری زیرساخت‌های فیزیکی برای طیف وسیعی از کاربران فراهم شد. در سال 2002 شرکت آمازون وب سرویس خود را ایجاد کرد که نقش مهمی در گسترش پردازی ابری داشت. این شرکت از سال 2006 امکان دسترسی به سامانه خود را از طریق وب سرویس‌های آمازون را بر پایه پردازش همگانی فراهم کرد. شرکت گوگل هم با ارایه سرویس ابری گوگل داکس در همان سال، خدمات ابری را به سطح عموم جامعه آورد و پس از آن شرکت‌های مختلف، خدمات متنوعی را بر بستر رایانش ابری فراهم کردند. (رادمنش، شیری، آیت، 1395)

محاسبات انبوه از دید فراهم کنندگان منابع زیر ساخت، می‌تواند با کمک ماشین‌های مجازی شبکه شده، به عنوان یک روش جدید برای ایجاد پویای نسل جدید مرکز داده، مورد استفاده قرار گیرد تا بتواند یک زیرساخت قابل انعطاف برای ارائه انواع مختلف خدمات محاسباتی و ذخیره‌سازی در اختیار داشته باشند. (ایزدی، فرج پهلو، رضایی شریف آبادی، 1400)

محیط‌های ابری فراگیر هستند و انتظار می‌رود که حداقل بخشی از چشم‌انداز فناوری آینده در سازمانی را میزبانی کنند. این تکنولوژی جایگزین با صرفه‌جویی در هزینه، در حال حاضر در دسترس اکثریت است. در برخی موارد، هر سازمان باید تصمیم‌گیری کند که آیا می‌خواهد از مزیت‌های ابر استفاده کند یا خیر. مصرف کنندگان به طور منظم متصمیم می‌گیرند که آیا عکس‌ها، موسیقی و فایل‌های خود را در سیستم محلی خود ذخیره کنند یا از ارائه دهندگان ابر استفاده کنند. بنابراین شما چه چیزی را انتخاب می‌کنید؟ پاسخ ساده نمی‌باشد. تمام این وابسته به نیازهای شما و منابع در دسترس شما است. (Sun, 2020)

2- مطالب اصلی

2-1 تعریف مسئله و بیان سؤال‌های اصلی تحقیق

گسترش و افزایش سرعت و همه‌گیری شبکه‌های مقیاس وسیع مانند اینترنت و تشدید روزافرون رقابت و تغییرات و ظهور نیازهای جدیدی همچون نیاز به ارتباطات روزافزون، به روزرسانی مداوم محتوای داده و اطلاعات، تحریک‌پذیری و انعطاف و ... را به وجود آورده است. تلاش برای درآورده کردن نیازهای جدید به بازگشت و بلوغ مدل قدیمی رایانش شبکه‌ای در قالب یک مدل جدید عرضه خدمات فناوری اطلاعات شده است. (موزونی، ناظری‌نژاد، 2019)

در منابع فارسی زبان از این مدل جدید با عبارت‌هایی چون «رایانش ابری» (با بک هزاوه، آبان و آذر ماه 1388) «محاسبات ابری» (حنیف خالقی، شهریورماه 1388) و «پردازش ابری» (هادی هرمزی، الهام هرمزی، آریا پوریا نسب، تیرماه 1390) یاد می شود. داده‌ها در هر جایی که ذخیره شده‌اند در معرض خطر حمله قرار دارند، لذا امنیت محاسبه ابری همه موضوعات محاسبه را تحت پوشش قرار می‌دهد. رایانش ابری یک محیط مجازیست که به استقلال داده‌ها از راه ابر نیاز دارد، لذا چندین نگرانی در ذخیره داده‌ها می‌تواند به وجود آید. اساسا کاربران نه جای دقیق داده‌های خود را می‌دانند نه جای ذخیره منابع دیگر. امروزه مفهومی با عنوان پردازش ابری (CloudComputing) مورد استفاده و استقبال همگان قرار گرفته که کمپانی‌های بزرگ در زمینه اینترنت با تئوری به جای ذخیره و پردازش روی سیستم‌های شخصی، بر روی سرورهای آنها انجام می شود و به این ترتیب سهولت در دسترسی در هر مکان و هر زمان و به هر اندازه و بر حسب نیاز کاربر با دریافت هزینه آن در اختیارش قرار می‌گیرد. (فولادیان، سربازی، 1400)

حال، با توجه به به‌روز بودن این تکنولوژی دغدغه ما ابتدا شناخت طرز کار این سیستم «فضای ابری» به عموم جامعه و سهولت استفاده از آن در درجه دوم ایجاد سیستم‌های بومی رایانش ابری در کشور عزیزمان و در نهایت تنظیم مقررات و قوانین حقوقی برای میزبانان بستر رایانش ابری و استفاده کنندگان از این بستر می‌باشد. (سلطانی فر، 1400)

قلمرو حقوق کیفری با ورود فن‌آوری‌های نوین، بسیار گسترش یافته است. فرآورده‌های فناوری اطلاعات و ارتباطات چون آثار دیداری و شنیداری، موضوع بسیاری از مقررات کیفری گشته‌اند. پیرو چنین تحولاتی است که مجرمان چون همیشه زودتر از قانون‌گذاران، شیوه جرائم ارتکاب جرم را دگرگون نموده و جرائم جدیدی را وارد قلمرو حقوق کیفری نموده‌اند. به دنبال وامنش به چنین جرائمی بود که قانون‌گذار ایران، مقررات جدیدی تصویب و به کارگیری فن‌آوری رایانه و آثار دیداری و شنیداری را – گاه به عنوان موضوع جرم و گاه به عنوان وسیله‌ای برای ارتکاب جرم – جرم‌انگاری نمود. (Kemp, 2018)

قانون جرائم رایانه ای در اجرای اصل 123 قانون اساسی ایران در سال 1388 به تایید شورای نگهبان رسید و تصویب گشت. این قانون مشتمل بر هشت فصل و 56 ماده است. (قانون مجازات اسلامی)

باید گفت که قانونگذار با توجه به گسترده شدن روز افزون فناوری اطلاعات و ارتباطات در صدد این بوده است تا قوانین را هم مطابق با علم روز به صورت پویا پیش ببرد و رفتار های شخصی زیان آور را جرم انگاری کرده و اشخاصی را که مرتکب این رفتار ها میشوند را مجازات نماید. (Kemp, 2018)

2-2 سابقه و ضرورت انجام تحقیق

اهمیت ملاحظات امنیتی در مورد توسعه و استفاده از سیستم های اطلاعاتی، هیچ وقت از رشد باز نمی‌ماند. در حقیقت، سیستم‌های اطلاعاتی امروزه، در همه جا توسط افراد، سازمانها، دولتها و سیستم‌ها مورداستفاده قرار میگیرند و واضح است که این امر منجر به از دست دادن مقادیر زیادی پول، زمان و سایر منابع می شود. درنتیجه، سازمانها ممکن است نه تنها مبالغ بسیاری را صرف تجهیزات امنیتی همچون دیواره آتش، سیستم های تشخیص نفوذ و ابزارهای رمزنگاری برای محافظت از آنها در برابر تهدیدات نمایند، بلکه با مشکلات زیادی برای ارزیابی بررسی‌های فناوری امنیتی مواجه هستند. به علاوه، این شرکتها موارد امنیتی سیستم‌های آن ها را نقض می‌کنند چراکه سازمانهایی که بهتر ریسک‌های سایبری را مدیریت می‌کنند، از سوی بازار رقابتی موردتقدیر قرار خواهند گرفت. (Subramanian, 2018)

در سال 1399، ربابه شاهی مقاله‌ای در یازدهمین کنفرانس ملی علوم و مهندسی کامپیوتر و فناوری اطلاعات درج کردند با نام بررسی مدل‌های ارزیابی ریسک امنیت اطلاعات و ارائه راهکارهای پیشنهادی در سیستم‌های رایانش ابری، که به نتیجه گیری، ایجاد مدیریت امنیت اطلاعات یکی از نیازهای ضروری شرکتها و سازمانهای ابری می‌باشد. ارزیابی ریسک، مکانیزمی مهم در چرخه مدیریت امنیت اطلاعات است. از طرفی، ارزیابی ریسک، درجه ریسک قبلی را مشخص کرده و امکان تصمیم گیری دقیق برای کاهش و مدیریت این ریسکها را فراهم می‌آورد. برای شرکتها جهت پذیرش یک فرایند به خوبی ساختاریافته و نظام مند جهت ارزیابی ریسک‌های امنیت اطلاعات جهت ارزیابی آن، اهمیت دارد. که هدف اصلی پژوهش، بررسی و مقایسه و مدل ریسک امنیت کمیتی برای سیستم های رایانش ابری بود چراکه این سیستم‌ها نشان دهنده فناوری مربوطه برای شرکت‌هایی است که هزینه را کاهش و نام تجاری سازمان را ارتقا میدهند. (شاهی، 1399)

در سال 1400، امیر یداللهی، لیلا مرتضوی فر، علی قرمزیان در نهمین کنفرانس ملی پژوهش های کاربردی در علوم برق و کامپیوتر و مهندسی پزشکی مقاله‌ای تحت نام معماری ایمن ابر برای شبکه‌های حسگر بی سیم پزشکی نوشته‌اند که به طور خلاصه به چالش مدیریت داده‌ها در شبکه‌های حسگر بی‌سیم برای نظارت بر بیمار پرداختند .یک معماری امن و مقیاس پذیر را پیشنهاد داده‌اند که فن آوری رایانش ابری را به صورت پویا در مقیاس منابع ذخیره سازی از طریق تهیه تقاضا مورد استفاده قرار می‌دهد .علاوه بر این، یک طرح ابتکاری امنیتی ارائه داده‌اند که تهدیدات امنیتی بالقوه برون سپاری داده‌های پزشکی را از بین می برد و ازمحرمانه بودن، یکپارچگی بدون دخالت بیماران و پزشکان اطمینان حاصل می‌کند. برای پیاده سازی سیاست های امنیتی پیچیده و پویا که برای برنامه های پزشکی ضروری است، یک کنترل دسترسی ریزدانه ای را ایجاد کرده‌اند که ترکیبی از رمزنگاری مبتنی بر ویژگی ها و رمزنگاری متقارن است. (یداللهی، مرتضوی‌فر، قرمزیان، 1400)

در May 2019، در 6 th International Conference On Information Technology, Computer & Telecommunication مرتضی موزونی و ابولفضل ناظری نژاد مقاله ای تحت نام ارزیابی چالشها و تهدیدات امنیتی در محاسبات ابر با تاکید بر امنیت ذخیره سازی داده و حفظ حریم خصوصی ارائه دادند که بصورت خلاصه میتوان نتیجه گرفت، محاسبات ابری به دلیل کارایی، دسترس پذیری، هزینه کم و چندین مزیت دیگر یک انقلاب در صنعت فناوری اطلاعات است. محاسبات ابری یک روش برای به حداکثر رساندن ظرفیت یا اضافه کردن امکانات بدون سرمایه گذاری در زیرساخت جدید، تربیت پرسنل جدید یا تهیه نرم‌افزار جدید است. مسئله این است که چرا سازمانها با وجود دامنه وسیعی از مزایا که محاسبات ابری ارائه می‌کنند، به قرار دادن کسب وکارشان در ابر بی میل هستند. امنیت داده در ابر یکی از موضوعات مهم است که به عنوان یک مانع در پیاده سازی محاسبات ابری عمل می‌کند. ایجاد یک معماری محاسبات ابری انعطاف‌پذیر و یکپارچه برای اشتراک انواع منابع هنوز با موانعی از جمله امنیت داده و حفظ حریم خصوصی رو به رو است، بنابراین تکنیک‌های امنیتی باید به گونه‌ای باشند که علاوه بر برآورده کردن امنیت، از لحاظ کارایی و عملیاتی نیز بهینه و قابل پیاده سازی باشند. پیشرفتهای روزافزون آن با سرعت فراوان، میتواند برای بهینه‌سازی و رفع نیازهای مختلف فناوری اطلاعات، کاربردهای بسیاری داشته باشد، از اینرو در آن مقاله به بررسی مسائل امنیتی به خصوص امنیت ذخیره‌سازی داده و حفظ حریم خصوصی در محیط محاسبات ابری پرداخته شد. (موزونی، ناظری‌نژاد، 2019)

2-3 مقدمه‌ای بر بحث حقوقی در ایران

قلمرو حقوق کیفری با ورود فن‌آوری‌های نوین، بسیار گسترش یافته است. فرآورده‌های فناوری اطلاعات و ارتباطات چون آثار دیداری و شنیداری، موضوع بسیاری از مقررات کیفری گشته‌اند. پیرو چنین تحولاتی است که مجرمان چون همیشه زودتر از قانون‌گذاران، شیوه جرائم ارتکاب جرم را دگرگون نموده و جرائم جدیدی را وارد قلمرو حقوق کیفری نموده‌اند. به دنبال وامنش به چنین جرائمی بود که قانون‌گذار ایران، مقررات جدیدی تصویب و به کارگیری فن‌آوری رایانه و آثار دیداری و شنیداری را – گاه به عنوان موضوع جرم و گاه به عنوان وسیله‌ای برای ارتکاب جرم – جرم‌انگاری نمود. (قانون مجازات اسلامی)

ماده 213 مکرر قانون مجازات عمومی 1304 برای اولین بار تجارت، توزیع و فروش اشیایی چون فیلم، نقاشی و تصویرهای جریحه‌دار کننده عفت عمومی را جرم شمرد. موضوع این ماده، طرح، گراور، نقاشی، تصاویر، مطبوعات، اعلانات، علائم یا فیلم سینما می‌باشد. هر چند، با افزوده شدن عبارت «به طور کلی هر شیء دیگری که عفت و اخلاق عمومی را جریحه‌دار نماید» قلمرو ماده گسترش یافت، اما تفسیر حقوقی درست نیازمند این است که دیگر اشیاء از جنس موارد گفته شده باشند. رفتارهای سه بند دیگر این ماده، اقداماتی چون توزیع، ساختن، وارد و صادر کردن و معامله، همچنین راهنمایی برای تحصیل اشیاء گفته شده می‌باشد. در ادامه ماده مقرر شده بود که «مفاد این ماده شامل اشائی نخواهد بود که از محصولات صنایع مستظرفه محسوب و یا جنبه علمی داشته و برای مقاصد علمی به اشخاصی که سن آنها

بیش از 18 سال است فروخته شده و یا در موزه به معرض انظار عموم گذارده می‌شـود» که اشـاره به برخی عوامل موجهه دارد. ماده 640 قانون مجازات اسـلامی، جایگزین ماده 213 مکرر قانون مجازات عمومی شـد و مجازات مرتکب را از شش ماه تا دو سال حبس به سه ماه تا یک سال حبس، جزای نقدی از یک میلیون و پانصد هزار ریال تا شش میلیون ریال و تا 74 ضربه شلاق تغییر داد. قلمرو رفتارهای مقرر در بندهای دوم و سوم گسترش یافت و به کار گیری عبارت‌های مبهم، بسـتر فقسـیرهای گوناگون از ماده را باز کرد. قسمت اخیر ماده نیز در شکل دو تبصره آورده شد. (قانون مجازات اسلامی)

با گسـترش ارتکاب این گونه از جرائم، قانون مجازات اشـخاصـی که در امور سمعی و بصری فعالیت‌های غیر مجاز می‌نمایند، مصوب 72، افرادی را مجرم شمرد که موضوع رفتار مجرمانه‌شان، آثار سمعی و بصری بود. قانون یاد شده، دارای پنج ماده و یازده تبصره و موضوع این قانون آثار سمعی و بصری مجاز و غیر مجاز بود. معرفی آثار غیرمجاز به جای مجاز و تضـییع حقوق صـاحبان اثر، موضـوع ماده یک این قانون بود. ماده دوم، نگرفتن مجوز لازم برای توزیع، تکثیر و عرضـه نوارهای صـوتی و تصـویری از وزارت فرهنگ و ارشاد اسلامی را جرم می شمرد. ماده سوم فعالیت‌های تجاری آثار سمعی و بصری غیر مجاز را جرم انگاری می‌نمود و در دو بند مقررات تو صیفی در این زمینه وضع شده بود. ماده چهارم رسیدگی به این جرائم را در صلاحیت دادگاه انقلاب قرار می‌داد. همچنین مسـئولیت کیفری اشـخاص حقوقی در ارتکاب چنین جرائمی پذیرفته نشده بود و بالاترین مقام اجرایی تصمیم‌گیری، مرتکب جرم شمرده می‌شد. به دنبال رویدادهای مجرمانه‌ای که با ارتکاب برخی از این جرائم رخ داد و عفت عمومی را به شدت جریحه‌دار کرد، در سال 1386 قانون یاد شده لغو و قانون دیگری (از این پس ق.س.ب نامیده می شود.) به صورت عجولانه تصـویب شـد که سـیاسـت سـرکوبگرانه شـدیدی را برای مقابله با مجرمان در پیش گرفت. قانون جدید قلمرو جدید قلمرو فعالیت‌های مجرمانه مربوط به امور سـمعی و بصـری را گسـترش و میزان مجازات‌ها را به شـدت افزایش داد. مجازات‌های قانون پیشین، جزای نقدی، شلاق و حبس و بود که حداقل هر کدام به ترتیب یک صد هزار ریال، یک ضربه و یک سال و حداکثر هر کدام به ترتیب یک صد میلیون ریال، هفتاد و چهار ضربه و ده سال حبس، همچنین مجازات مفسد فی الارض بود. در قانون جدید حداقل مجازات عبارت است از دو میلیون ریال جزای نقدی، سی ضربه شلاق و یک روز و سه ماه حبس و حداکثر دویست میلیون ریال جزای نقدی، هفتاد و چهار ضربه شلاق و ده سال حبس. همچنین در مواردبسیار مجازات مفسد فی الارض پیش‌بینی شده است. محرومیت ده ساله از حقوق اجتماعی نیز در برخی موارد این قانون به چشم می‌خورد. در ماده یک پیشین عبارت «هر شخصی» به کار رفته بود که در قانون جدید عبارت «هر شـخص حقیقی یا حقوقی» به کار رفته اسـت. در ماده سـه به تولید آثار مسـتهجن با عنف و اکراه و به منظور سـوء اسـتفاده جنسی دیگران اشاره شده است. علاوه بر مواردی چون فیلم، نوار و دیسک که دوباره موضوع فعالیت‌های مجرمانه قرار گرفته، لوح‌های فشرده نیز به فهرست این قانون افزوده شده است. مواد چهارم به بعد، رفتارهای مجرمانه جدیدی را جرم می شمارد. تهدید به افشاء آثار مستهجن و انجام زنا با دیگری موضوع ماده چهار اسـت. وسـیله تهدید قرار دادن آثار مسـتهجن، وسـیله هر منظور نام‌شروع قرار دادن آنها. تهیه فیلم یا عکس از مکان اختصاصی بانوان، تهیه، تکثیر و توزیع فیلم یا عکس مبتذل از مراسـم خانوادگی دیگران، جرائم ماده پنج می‌باشند. نوآوری دیگر این قانون در ماده شش است که رابطه زوجیت را مانع اعمال مجازات جرم تکثیر، انتشار یا توزیع عمده اثر نمی‌داند. در خصوص مطالبه ضـرر و زیان هم بر خلاف قانون قدیم، صـلاحیت دادگاه کیفری رسیدگی کننده و دادگاه محل اقامت بزه دیده را به رسمیت می‌شناسد. در ماده هشت نیز سوء استفاده مأموران دولتی که بنابر اقتضاء شغلی، آثار مستهجن در اختیارشـان قرار می‌گیرد را جرم می‌داند. به کارگیری ارتباطات الکترونیکی و سایت‌های کامپیوتری برای انتشار آثار مستهجن نوآوری مقرر در ماده ده قانون س.ب است.

در راسـتای چنین مقرراتی، برای پاسـخ به نیاز مردم جهت تجارت در بسـترهای ایمن الکترونیکی، قانون تجارت الکترونیکی در سـال 1382 با هشتاد و یک ماده و هفت تبصره به تصویب مجلس شورای اسلامی رسید. باب چهارم آن که دارای چهار مبحث اسـت به جرائم و مجازات‌ها اختصـاص دارد و جرائمی چون کلاهبرداری و جعل رایانه‌ای را جرم می‌داند. البته موضوع جرائم این قانون آثار سمعی و بصری مبتذل یا مستهجن نمی‌باشد بلکه درباره ارتکاب جرم در بستر مبادلات الکترونیکی است. ماده یک هم درباره چهارچوب این قانون مقرر می‌دارد: «این قانون مجموعه اصول و قواعدی است که برای مبادله آسـان و ایمن اطلاعات در واسـط‌های الکترونیکی و با اسـتفاده از سیستم‌های ارتباطی جدید به کار می‌رود». بر این اساس، به جز تعامل اندکی که با قانون جرائم رایانه‌ای دارد، از قلمرو برسـی این مقاله بیرون اسـت. برای تکمیل ضـمانت اجراهای کیفری این قانون، قانون جرائم رایانه‌ای (از این پس ق.ج.ر نامیده می‌شـود) به عنوان فصـل جدیدی به قانون مجازات اسـلامی افزوده شد که آثار سمعی و بصری را موضوع برخی مقررات خود قرار داد و در ادامه، به کارگیری فن‌آوری‌های نوین برای ارتکاب برخی از جرائم سنتی چون سـرقت، کلاهبرداری و جاسـوسـی را جرم‌انگاری نمود. این قانون دارای سـه بخش است که پنجاه و شش ماده تصویب شده است. بخش اول درباره جرائم و مجازات‌هاسـت. جرائمی چون شـنود غیرمجاز، جاسـوسـی و جعل رایانه‌ای، تخریب و ... در این بخش جرم‌انگاری شـده‌اند که می‌توان آنها را جرائم رایانه‌ای نامید. جرائم رایانه‌ای به جرائمی گفته می‌شود که در آن رایانه، وسیله، هدف یا واسـط ارتکاب جرم اسـت و گاهی علیه اموال، گاهی علیه تمامیت مجازی اشـخاص و بعضـی وقت‌ها علیه نرم‌افزار، سـخت‌افزار و داده و برضـد آسایش و امنیت عمومی است (انیسی حماسه، 89، ص49). بخش دوم درباره آیین دادرسـی کیفری این گونه از جرائم اسـت. بخش سـوم نیز دیگر مقررات مربوط را در خود جای داده است. فصل چهارم از بخش اول درباره جرائم علیه عفت و اخلاق عمومی و فصـل پنجم درباره هتک حیثیت و نشـر اکاذیب می‌باشـد که تعامل گسـترده‌ای با ق.س.ب دارد. مهم‌ترین نوآوری این قانون، پذیرش آشکار مسئولیت کیفری اشخاص حقوقی است. یعنی افزون بر مجازات شـخص حقیقی مرتکب جرم، چنانچه جرم در راسـتای منافع شـخص حقوقی ارتکاب یابد، شـخص حقوقی دارای مسـئولیت کیفری خواهد بود. (قانون مجازات اسلامی)

2-4 قانون جرائم رایانه ای

قانون جرائم رایانه ای در اجرای اصل 123 قانون اساسی ایران در سال 1388 به تایید شورای نگهبان رسید و تصویب گشت. این قانون مشتمل بر هشت فصل و 56 ماده است. (قانون مجازات اسلامی)

در فصل یکم این قانون عنوان جرائم علیه محرمانگی داده ها و سیستم های رایانه ای و مخابراتی بررسی میشود.

ماده1ـ هرکس به طور غیرمجاز به داده ها یا سامانه های رایانه ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون (5.000.000) ریال تا بیست میلیون (20.000.000) ریال یا هر دو مجازات محکوم خواهد شد. (قانون مجازات اسلامی)

در این خصوص باید بگوییم که رفتار فیزیکی در این جرم فعل دسترسی غیر مجاز به داده ها یا سامانه های رایانه ای یا مخابراتی میباشد. در این خصوص باید توجه داشت که دسترسی به داده ها یا سامانه های رایانه ای و مخابراتی صرفا باید صورت بگیرد و اینکه که ان داده ها و سامانه های رایانه ای یا مخابراتی باید با تدابیر امنیتی حفاظت بشوند به بیان دیگر ان دسته از داده ها و سامانه های رایانه ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت نمی شوند شامل این ماده نیستند. پس همانطور که ملاحظه میشود چنانچه بخواهیم از عنوان این ماده جهت به مجازات رساندن فرد یا افرادی استفاده کنیم باید این داده ها تحت محافظت و تدابیر امنیتی باشند و داده هایی که تحت تدابیر محافظتی نباشند را شامل نمیشود. در هر حال باید گفت که این جرم از جمله جرایم مطلق است و نیازی به نتیجه ندارد یعنی صرف دسترسی پیدا کردن به داده ها یا سامانه های رایانه ای و مخابراتی صرف نظر از ایجاد نتیجه جرم است. (قانون مجازات اسلامی)

ماده2ـ هر کس به طور غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی در سامانه های رایانه ای یا مخابراتی یا امواج الکترو مغناطیسی یا نوری را شنود کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ده میلیون (10.000.000) ریال تا چهل میلیون (40.000.000) ریال یا هر دو مجازات محکوم خواهد شد.

عنوان جرم در این ماده شنود غیر مجاز است . همانطور که مشخص است شنود باید به طور غیر مجاز انجام گیرد یعنی فرد مجوزی برای این امر نداشته باشد. شرط دیگری که برای تحقق عنصر مادی این جرم لازم است این است که محتوایی که مورد شنود غیر مجاز قرار می گیرد در حال انتقال باشد یعنی وقتی این محتوای ارتباطات غیر عمومی در حال انتقال هستند توسط متهم به طور غیر مجاز شنود شوند . محتوای ارتباطات غیر عمومی باید شنود شوند یعنی اگر ارتباطات عمومی باشد و توسط فردی شنود شود متهم را نمی توان بر طبق این ماده مجازات کرد پس لازم است محتوای در حال انتقال ارتباطات غیرعمومی شنود شود. ضمنا این شنود باید در سامانه های رایانه ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری انجام گیرد در غیر این صورت شامل این ماده نمی شود. این جرم نیز از جرایم مطلق بوده و نیازی به تحقق نتیجه خاصی ندارد و صرف اینکه و همین که محتوای در حال انتقال ارتباطات غیر عمومی در سامانه های رایانه ای یا مخابراتی یا امواج الکترو مغناطیسی یا نوری مورد شنود قرار گیرد برای تحقق این جرم کافی است. (قانون مجازات اسلامی)

در مواد دیگر نیز رفتار های مجرمانه دیگری در همین ارتباط تعریف شده است.

باید گفت وجه مشترک آنها در این است که از جرائم مطلق بشمار میروند. به این معنا که صرف انجام آنها منجر به تحقق جرم میشود و نیازی نیست نتیجه حاصل گردد. فرض کنید شخصی عکسهای فرد دیگری را سرقت میکند و قصد آن را دارد تا در شبکه های مجازی جهت افزایش فالوور پخش کند اما به هر دلیلی موفق به پخش آن نمیشود . در اینجا صرف سرقت داده ها با این قصد کفایت میکند تا جرم محقق شود و نیازی نیست تا نتیجه جرم هم حاصل میشد. (قانون مجازات اسلامی)

رشد در رایانش ابری عمومی موجب افزایش نیاز به امنیت بیشتر شده ا ست. سرویس‌های ابر عمومی نیاز به فراهم کردن سرویس‌های مؤثر از نظر هزینه و مجموعه‌ای از ویژگی‌ها که امکان انتخاب را آسان می‌کند، دارند اما برآورده کردن الزامات IT به گونه‌ای ایمن نیز بسیار اهمیت دارد. در این فصل سوالاتی امنیتی برای راهنمایی خوانندگان در توسعه لیست‌های خود برای ارزیابی امنیت ابر خصوصی و عمومی داده شده است. و همچنین از دید حقوقی در ایران باید گفت که قانونگذار با توجه به گسترده شدن روز افزون فناوری اطلاعات و ارتباطات در صدد این بوده ا ست تا قوانین را هم مطابق با علم روز به صورت پویا پیش ببرد و رفتار های شخصی زیان آور را جرم انگاری کرده و اشخاصی را که مرتکب این رفتار ها میشوند را مجازات نماید. به همین منظور قانون جرائم رایانه ای پیش بینی و تصویب شد. با تمام ایراداتی که میتوان نسبت به این قانون گرفت اما قدم مثبتی بود تا افراد سودجو در شبکه های مجازی و بطور کلی در فضای بسیار گسترده فناوری اطلاعات و ارتباطات به مجازات و کیفر قانونی اقدامات خود برسند.

در کل میتوان گفت که ابزار کیفری در صورتی مفید است که به نحو دقیق و همراه با مطالعه و در راستای فردی کردن مجازات مجرمان سایبری باشد. از نقاط ضعف این قانون نیز میتوان گفت که تعیین حبس یا جزای نقدی یا هردو به عنوان مجازات مجرمان جرائم رایانه ای و عدم تناسب میان جرم و مجازات از نقاط ضعف آن است. امید است تا در آینده قانونگذار برای تقویت کارایی این قانون حین تصویب قانون جدید مجازات اسلامی در رفع خلاء و نارسایی های آن اقدامات موثر و سازنده ای را بعمل آورد و موجبات پیوستن ایران به معاهدات بین المللی پیشگیری و مبارزه با جرائم سایبری را فراهم آورد .

3- نتیجه گیری

شبکه های رایانش ابری به علت سادگی و کارابودن مورد پذیرش شرکت‌های بزرگ برای نیازهای روزمره واقع شده اند که در این شبکه‌ها مسئله مهم جستجو و تشخیص پردازنده مناسب برای ارجاع به درخواست آنها می‌باشد. و چنانچه بتوان با استفاده از مجازی سازی که قابلیت به اشتراک گذاری و انحصاری کردن داده‌ها را فراهم کرد، میتوان از این تکنولوژی استفاده کرد و منجر به کاهش خطاها و هزینه‌ها شد. شایان ذکر است در آینده با راهکارو روش‌های مدیریتی در این زمینه با استفاده از مدل امنیتی مناسب می‌توان شبکه‌های رایانش ابری مناسبی ایجاد کرد. ایجاد مدیریت امنیت اطلاعات یکی از نیازهای ضروری شرکتها و سازمانهای ابری می‌باشد. ارزیابی ریسک، مکانیزمی مهم در چرخه مدیریت امنیت اطلاعات است. از طرفی، ارزیابی ریسک، درجه ریسک قبلی را مشخص کرده و امکان تصمیم گیری دقیق برای کاهش و مدیریت این ریسکها را فراهم می‌آورد. برای شرکتها جهت پذیرش یک فرایند به خوبی ساختاریافته و نظام مند جهت ارزیابی ریسک‌های امنیت اطلاعات جهت ارزیابی آن، اهمیت دارد. هدف اصلی این پژوهش، بررسی و مقایسه و مدل ریسک امنیت کمیتی برای سیستم‌های رایانش ابری است چراکه این سیستم‌ها نشان دهنده فناوری مربوطه برای شرکتهایی است که هزینه را کاهش و نام تجاری سازمان را ارتقا می‌دهند. همانطور که قبلاً اشاره شد مهمترین چالش رایانش

ابری تضمین امنیت داده های موجود می‌باشد. در حال حاضر حفاظت از کارکرد ابر در اینترنت یک چالش بزرگ محسوب می‌شود و راه حل های بسیاری برای امنیت داده‌ها در رایانش ابری به کار گرفته می‌شود. روش های گوناگونی جهت مقابله با حمله‌های احتمالی ابداع شده‌اند به نحوی که ارائه دهندگان ابر از بابت حفاظت داده‌های شخصی و سازمانی کاربران آسوده باشند. اما این روش ها کامل نیستند. سیستمی که بتواند در مقیاس های بزرگتر به طرز مناسب و کارآمد کار کند، مقیاس پذیر است. این ویژگی باعث می‌شود عملکرد کلی با افزودن منابع سخت افزاری افزایش یابد.

سپاسگزاری

بسیار سپاسگذارم از استاد گرامی جناب آقای دکتر احمد فراهی که داسوزی و تلاش و کوشش ایشان در تعلیم و تربیت و انتقال معلومات و تجربیات ارزشمند در کنار برقراری رابطه صمیمی و دوستانه با دانشجویان و ایجاد فضایی دلنشین برای کسب علم و دانش و درک شرایط دانشجویان حقیقتا قابل ستایش ا ست. اینجانب بر خود وظیفه میدانم در ک سوت شاگردی از زحمات ارزشمند شما استاد گرانقدر تقدیر و تشکر نمایم. از خداوند متعال برایتان سلامتی، موفقیت و همواره یاد دادن را مسئلت دارم.

مراجع

[1] ایزدی، عبدالرضا – فرج پهلو، عبدالحسین – رضایی شریف آبادی، سعید (1400) «ارائه مدلی جهت طراحی و پشتیبانی از پیاده‌سازی آرشیو ابری ملی ایران» مقاله علمی پژوهشی / ISC

[2] چاوشی، نیر – میرعابدینی، سیدجواد (1399) «مروری بر امنیت قراردادهای هوشمند در سیستم‌های مقیاس وسیع ساخت و ساز با رایانش ابری» مقاله علمی پژوهشی / ISC

[3] حسین زاده شبستری، رضا (1400) «یارانش ابری و بررسی بهبود امنیت در مهندسی کامپیوتر» اولین کنفرانس مکانیک، برق، مهندسی هوافضا و علوم مهندسی

[4] رادمنش، نگین – شیری، محمد براهیم – آیت، سید سعید (1395) «مروری بر امنیت محیط‌های رایانش ابری و انواع سیستم‌های تشخیص نفوذ ابری» نخستین کنگره بین‌المللی چالش‌های الکترونیکی تهران

[5] سلطانی فر، مهدی – زرگر، سید محمد (1400) « ارزیابی و رتبه بندی ریسک‌های امنیتی رایانش ابری بر اساس یک رویکرد ترکیبی مبتنی بر مقایسه های زوجی» مقاله علمی پژوهشی / ISC

[6] شاهی، ربابه (1399) « بررسی مدلهای ارزیابی ریسک امنیت اطلاعات و ارائه راهکارهای پیشنهادی در سیستمهای رایانش ابری» یازدهمین کنفرانس ملی علوم و مهندسی کامپیوتر و فناوری اطلاعات

[7] فولادیان، مجید – سربازی، مهدی (1400) «بررسی خدمات ابر دولتی در کشورهای مختلف، مطالعه موردی (استرالیا – انگلیس و آمریکا)» پنجمین همایش بین‌المملی دانش و فناوری ممهندسی برق کامپیوتر و مکانیک ایران

[8] موزونی، مرتضی – ناظری‌نژاد، ابوالفضل (2019) «ارزیابی چالشها و تحدیدات امنیتی در محاسبات ابر با تاکید بر امنیت ذخیره‌سازی داده و حفظ حریم خصوصی» 6 th International Conference on Information Technology, Computer & Telecommunication

[9] یداللهی، امیر – مرتضوی فر، لیلا – قرمزیان، علی (1400) «معماری ایمن برای شبکه‌های حسگر بی‌سیم پزشکی» نهمین کنفرانس ملی پژوهش‌های کاربردی در علوم برق و کامپیوتر و مهندسی پزشکی

[10] Kemp, Richard (2018) “Legal aspects of cloud security” Computer Law & Security Review

[11] Subramanian, Nalini (2018) “Recent security challenges in cloud computing” School of Computing, Sathyabama Institute of Science and Technology, Chennai, India

[12] Sun, Pan Jun (2020) “Security and privacy protection in cloud computing: Discussions and challenges” Journal of Network and Computer Applications