حقوق مالکیت فکری و رایانش ابری

ویژه‌نامه روزجهانی مالکیت فکری

همکاران سیستم

کمیسته ایرانی اتاق بازرگانی بین‌المللی

حقوق مالکیت فکری و رایانش ابری

ویژه‌نامه روزجهانی مالکیت فکری

با همکاری کمیته ایرانی اتاق بازرگانی بین‌المللی

همکاران طرح:

– فرید فولادی

عضو هیئت مدیره و معاون توسعه بازار شرکت همکاران سیستم

– دکتر علیرضا مسعودی

مشاور دفتر حقوقی شرکت همکاران سیستم

– دکتر شقایق بهشتی

مشاور دفتر حقوقی شرکت همکاران سیستم

– پریسا محمدخانی

کارشناس ارشد حقوق مالکیت فکری

– سینا حسن پور

مدیر پشتیبانی فنی شرکت همکاران سیستم

– دکتر مسعود ستوده

مدیر پروژه بازاریابی شرکت همکاران سیستم

– مریم حسینی

مدیر پروژه بازاریابی شرکت همکاران سیستم؛

– طراحی و صفحه‌آرایی

استودیو دیزاین همکاران سیستم

زمان انتشار: اردیبهشت ۱۳۹۸

فهرست

رایانش ابری چیست؟

شاید اصطلاح «رایانش ابری» چند سال گذشته، مفهوم پیچیده و دور از دسترسی را برای ما تداعی می‌کرد و گمان می‌کردیم با این تکنولوژی فاصله‌ی بسیاری داریم؛ اما امروز، اگر نگاه دقیقی به اطراف خود داشته باشیم، حضور این فناوری را در همه‌ی ابعاد زندگی خود می‌بینیم. ایمیل‌ها، حساب‌های کاربری در سرویس‌های مختلف، حافظه‌های ابری و حتی دفترچه‌ی تلفن موبایل ما هم، با فناوری رایانش ابری کار می‌کند و این موضوع، نقش پررنگ رایانش ابری را در زندگی روزمره‌ی ما نشان می‌دهد.

در یک تعریف عمومی، به استفاده از منابع پردازشی مانند سرورها، فضای ذخیره‌سازی و برنامه‌های کاربردی به شکل برخط، رایانش ابری می‌گویند. در این روش شرکت‌های ارائه‌دهنده‌ی خدمات ابری با تهیه زیرساخت‌ها و تجهیزات لازم، این منابع را به شکل متمرکز و به عنوان سرویس در اختیار شرکت‌ها، سازمان‌ها و افراد قرار می‌دهند. بنابراین، شرکت‌هایی که امکانات و تجهیزات لازم برای ارائه‌ی خدمات رایانش ابری را دارند، «شرکت ارائه‌دهنده‌ی خدمات ابری» نامیده می‌شوند. به شرکت‌ها، سازمان‌ها و افرادی که از خدمات ابری این شرکت‌ها استفاده می‌کنند نیز «مشتری خدمات ابری» یا «کاربر ابر» می‌گویند.

شیوه‌ی کار به‌این شکل است که مشتریان، با استفاده از اینترنت یا سایر شبکه‌های ارتباطی، به منابع پردازشی متصل شده و از آن استفاده می‌کنند. در این مدل مالکیت داده‌ها متعلق به مشتری است و مشتری می‌تواند در هر زمانی که بخواهد، به داده‌های خود دسترسی داشته باشد؛ ارائه‌دهنده خدمت نیز وظیفه دارد طبق توافق‌نامه سطح خدمات[1] از داده‌های مشتری نگه‌داری و دسترسی به داده‌ها و منابع پردازشی را برای وی فراهم کند.

مدل‌های بکارگیری رایانش ابری

مدل‌های بکارگیری رایانش ابری شامل موارد زیر است:

- **ابرهای عمومی:**

در این روش، مالکیت زیرساخت و منابع محاسباتی در اختیار یک شرکت است و از طریق شبکه عمومی، خدمات خود را ارائه می‌کند. در این نوع ابر، برنامه‌های مشتریان مختلف در سرورها و سیستم‌های ذخیره‌ساز و شبکه ابری باهم قرار دارند.

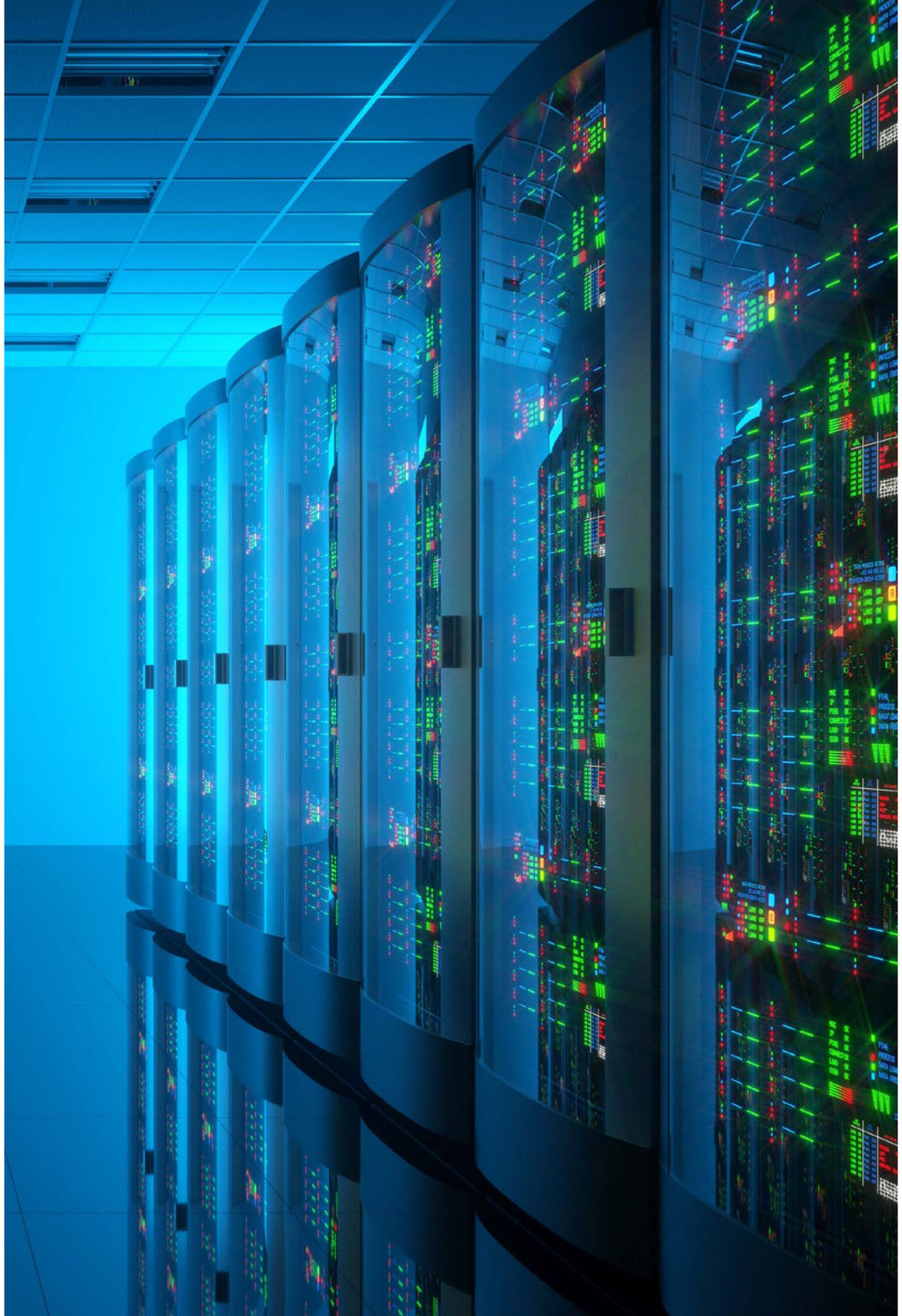
- **ابر خصوصی:**

در مقابل تعریف ابرهای عمومی، ابرهای خصوصی قرار دارند که زیرساخت آن در داخل یک واحد تجاری و یا سازمان قرار دارد و در دسترس عموم نیست. به بیان دیگر، ابر خصوصی به معنی طراحی یک زیرساخت محاسباتی با اضافه کردن مجازی‌سازی و واسط‌های مشابه ابر است. این ساختار به کاربران اجازه می‌دهد تا با دیتاسنترهای محلی خود تعامل داشته باشند. در واقع ابر خصوصی، مراکز داده مجازی شده داخل فایروال[2] شرکت هستند. در این مدل اغلب مصرف‌کننده و فراهم‌کننده ابر یکی هستند؛ البته ممکن است این فضا در مرکز داده شرکت دیگری باشد که به آن ابرخصوصی برون سازمانی می‌گویند.

- **ابر ترکیبی:**

به روشی که در آن چند ابر ارتباط دارند (انجمنی، خصوصی یا عمومی) ابر ترکیبی گفته می‌شود. به عنوان مثال ممکن

1. Service Level Agreement (SLA) 2. Firewall



است سازمانی برای نیازهای اصلی خود مانند سرور اصلی وب‌سایت از ابر خصوصی استفاده کند ولی برای برخی کاربردها مانند کار با فایل‌های چندرسانه‌ای با ترافیک بالا از ابر ترکیبی استفاده نماید. یک ابر ترکیبی، متشکل از چندین فراهم‌کننده ابر است. این ارائه‌دهندگان به صورت مؤسسات جدا هستند ولی به واسطه فناوری استاندارد که امکان جابجایی و انتقال داده و برنامه را فراهم می‌کند، اتصالاتی محدود دارند.

مدل‌های ارائه خدمات در رایانش ابری

خدمات رایانش ابری را می‌توان در سه گروه عمده تقسیم‌بندی کرد:

- **زیر ساخت به عنوان خدمت یا به اختصار IaaS:**[3]

پایه‌ای‌ترین خدمات زیرساخت مانند تهیه سرور، پردازنده، فضای ذخیره‌سازی و دیگر منابع بر حسب نیاز در این مدل ارائه می‌شود. در حال حاضر غالب خدماتی که تحت فناوری رایانش ابری در داخل کشور ارائه می‌شود از این نوع است.

- **بستر به عنوان خدمت یا به اختصار PaaS:**[4]

این خدمات شامل نرم‌افزار و سرویس‌هایی است که به کاربران اجازه می‌دهد با استفاده از ابزارهای عرضه شده توسط ارائه‌دهنده، برنامه‌های کاربردی و نرم‌افزار تولید کنند. این خدمات می‌تواند شامل ویژگی‌های از پیش پیکربندی شده‌ای باشد که مشترکین می‌توانند به عضویت آن در بیایند و از آن‌ها استفاده کنند.

- **نرم‌افزار به عنوان خدمت یا به اختصار SaaS:**[5]

خدمات این گروه تنوع زیادی دارند؛ چرا که بیشتر خدمات ارائه شده از یک برنامه کاربردی می‌تواند تحت عنوان خدمات نرم‌افزاری در اختیار کاربر قرار گیرد. در این روش کاربر با یک حساب کاربری و بر بستر اینترنت می‌تواند از نرم‌افزار استفاده کند. همچنین به‌روزرسانی و نگهداری این نرم‌افزارها به عهده ارائه دهنده خدمت است.

3. Infrastructure as a service 4.Platform as a service 5. Software as a Service

جمع‌بندی

در چند سال اخیر استقبال از این فناوری در بازار راهکارهای سازمانی افزایش یافته و عرضه‌کنندگان، علاوه بر روش‌های معمول، راهکارهای خود را بر بستر این فناوری نیز فراهم کرده‌اند. با گسترش استفاده از رایانش ابری، اهمیت توجه به مسئولیت ارائه‌دهندگان این خدمات و استفاده‌کنندگان آن در مورد داده‌ها بیشتر شده است. در این ویژه‌نامه موضوعات حقوق مالکیت فکری و موضوعات فنی رایانش ابری مورد بررسی قرار خواهد گرفت.

> **به استفاد از منابع پردازشی مانند سرورها، فضای ذخیره‌سازی و برنامه‌های کاربردی به شکل برخط، رایانش ابری می‌گویند.**

چالش‌های حقوقی رایانش ابری

چالش‌های حقوقی رایانش ابری از دیدگاه‌های مختلف قابل بررسی است. مواردی که برای انعقاد قراردادهای رایانش ابری باید بین ارائه‌دهنده‌ی خدمات ابر و مشتری رعایت شود؛ امنیت داده‌های مشتریان و مسئولیت ارائه‌دهنده در حفاظت از آن؛ جرائم سایبری متعدد از قبیل هک‌کردن و نفوذ به سیستم ارائه‌دهنده و قانون حاکم بر محیط ابر، از جمله موضوع‌های چالش‌برانگیز حقوقی محسوب می‌شود. همچنین حقوق مالکیت فکری و حمایت از صاحبان این حقوق در محیط‌های ابری از جمله مسائلی است که در رایانش ابری اهمیت دارد. مسئله‌ی دیگر این است که در بسیاری از کشورها قانونی در حوزه‌ی رایانش ابری به تصویب نرسیده و رویه‌ی قضایی واحدی نیز در رسیدگی به دعاوی این حوزه وجود ندارد که مقابله با این چالش‌ها را دشوار می‌کند.

دامنه‌ی پیچیدگی‌های حقوقی مرتبط با ابر حتی بر قوانین دادرسی نیز تأثیر می‌گذارد. همان‌طور که اشاره شد، طبیعت ابر، مجازی و غیرفیزیکی است و یکی از جنبه‌های رایانش ابری، فقدان محل دقیق[6] است. خدمات ابری ممکن است به کاربری در حوزه‌ی قضایی معینی فروخته شود ولی این امکان وجود دارد که داده‌های آن کاربر در محل واحدی ذخیره نشده و در چند نقطه در همان حوزه‌ی قضایی یا در حوزه‌های قضایی دیگر ذخیره و پردازش شود. ممکن است کاربر ـمشتریـ نیز هیچ اطلاعی نداشته باشد که داده‌هایش در کجا ذخیره یا پردازش می‌شود. علاوه‌براین، ممکن است داده‌ها در حین ذخیره، جداسازی شوند و حتی در زمان‌های مختلف در کشورهای مختلفی ذخیره شوند. بدین‌ترتیب تشخیص اینکه داده‌ها در یک زمان معین در کجا ذخیره شده‌اند برای کاربر مشکل می‌شود. مراحل مختلف پردازش داده‌ها نیز می‌تواند در حوزه‌های قضایی مختلف انجام شود.

ذکر همین چند مثال کافی است تا دشواری تعیین قانون حاکم بر محیط ابری را دریابیم. البته این دشواری در حقوق مالکیت فکری بیش‌تر می‌شود، زیرا حقوق مالکیت فکری در یک محدوده‌ی جغرافیایی و کشور معین اجرا می‌گردد و در بسیاری موارد واضح نیست که در محیط ابری قوانین مالکیت فکری کدام کشور باید اعمال شود.

به نظر می‌رسد که برای تعیین قانون حاکم بر محیط ابری باید از تمام گزینه‌هایی که می‌توانند به‌عنوان معیار تعیین قانون حاکم انتخاب شوند، گزینه‌ای را انتخاب کرد که نسبت به سایر گزینه‌ها اساسی‌تر است. برای مثال تابعیت شرکت، محل ذخیره‌سازی و محل پردازش، سه گزینه در تعیین قانون حاکم هستند؛ اما معیار اساسی‌تر و تعیین‌کننده‌تر را باید در روابط مشتری و ارائه‌دهنده و شرایط فعلی قانون‌گذاری در جهان جست‌وجو کرد. از آنجا که تابعیت ارائه‌دهنده برای مشتریان شناخته شده است ـدرحالی‌که محل ذخیره‌سازی و پردازش لزوما شناخته‌شده نیستـ و مشتریان با توجه به قوانین و شرایط کشور متبوع ارائه‌دهنده به انعقاد قرارداد اقدام می‌کنند، می‌توان قانون حاکم بر محیط ابری را همان قانون کشور متبوع شرکت ارائه‌دهنده دانست، چراکه در حال حاضر امکان همکاری بین کشورها در تدوین قانون واحد برای محیط ابری امکان‌پذیر نیست. البته شایان ذکر است که این موارد باید در قرارداد بین مشتری و ارائه‌دهنده تصریح شود تا هنگام بروز اختلاف، بتوان به سادگی تعیین تکلیف کرد.

6. Lack of a Clear Locality

در ادامه به بررسی برخی از چالش‌های حقوقی رایانش ابری خواهیم پرداخت.

۱. امنیت داده‌ها در ابر: خطرها و شرایط مقابله با آن‌ها

با وجود اینکه ابر در کسب‌وکار به شرکت‌ها کمک می‌کند، اما نسبت به اطلاعات حساس بخصوص در حوزه مالکیت فکری، خطرهایی دارد. از جمله‌ی این موارد می‌توان از حملات مجرمان سایبری به سیستم‌های ابری، سرقت اطلاعات و دیگر موارد ناقض امنیت نام برد. طبق گزارش پایگاه اینترنتی وریزون که در سال ۲۰۱۴ درخصوص رسیدگی به نقض داده‌ها منتشر شد، بیش از یک‌چهارم مجرمان سایبری، حوزه‌ی مالکیت فکری را هدف گرفته و به‌عبارتی جاسوسان مالکیت فکری هستند. همچنین طبق گزارش دیگری که در سال ۲۰۱۲ از وریزون منتشر شد جاسوسان مالکیت فکری[7] بیش‌تر افراد تحصیل کرده هستند.

اما این نکته شایان توجه است که افشای داده‌ها همیشه هم به دلیل سوءنیت نیست. برای مثال این امکان وجود دارد که کارمند شرکت، تبلت خود را در تاکسی جا بگذارد و اسرار تجاری شرکت، که در ایمیل یا پوشه‌ی دانلودهای تبلت کارمند موجود است، به دست رقبا بیفتد و بدین‌صورت اطلاعات از دست برود. طبق یافته‌های یک نظرسنجی که مایکروسافت در سال ۲۰۱۲ انجام داد، تقریبا هفتاد درصد از صاحبان مشاغل در سرتاسر آمریکا از موبایل شخصی خود برای کار و دسترسی به ابر استفاده می‌کرده‌اند، چه شرکت‌شان اجازه‌ی آن را بدهد چه ندهد. با این شرایط شکی نیست که برخی دستگاه‌ها ممکن است گم شوند، یا حساب‌های ایمیل باز بمانند و پیوست‌ها به‌طور تصادفی ارسال شوند.

اینک این سؤال مطرح است که چگونه می‌توان با این خطرها مقابله کرد؟ شاید بتوان در وهله‌ی اول بهترین راه را در پیش‌گیری از بروز خطر جست‌وجو کرد. اگر بتوان با استفاده از راهکارهای فنی از نفوذ مجرمان سایبری ممانعت به عمل آورد، بخش بزرگی از امنیت داده‌ها تأمین خواهد شد.

رمزگذاری[8] راهکاری است که با جلوگیری از دسترسی اشخاص غیرمجاز به داده‌ها، امنیت آن‌ها را تأمین می‌کند. در صورت اتخاذ این تدبیر، داده‌ها ـچه در یک پوشه‌ی ابر باشند، چه در لینک یک ایمیلـ برای هر شخصی قابل دسترس نبوده و دیگر اهمیتی ندارد چه کسی تبلت را در تاکسی پیدا کند.

۲. حقوق مالکیت فکری در ابر

حقوق مالکیت فکری از کشوری به کشور دیگر متفاوت است. بنابراین، مشتریان خدمات ابری باید با آگاهی کامل از قوانین و مقررات کشوری که قصد استفاده از خدمات آن را دارند، وارد این عرصه شوند و بدانند که ارائه‌دهنده بر اساس چه قوانینی و چگونه از حقوق آنها محافظت می‌کند.

• حق اختراع:[9]

ارتباط اختراع با رایانش ابری را می‌توان در نرم‌افزارها، سخت‌افزارها یا فرآیندهایی جست‌وجو کرد که برای پردازش و ذخیره‌سازی داده‌ها در رایانش ابری اختراع شده‌اند و حق اختراع دارند. در این صورت بکارگیری این فرآیندها، نرم‌افزارها و سخت‌افزارها در سیستم‌های ارائه‌دهنده، مستلزم کسب اجازه از صاحب حق اختراع و انعقاد قراردادهای لایسنس است، در غیر این صورت نقض حق اختراع رخ داده است. همچنین، امکان دارد که شخص ثالثی بدون کسب اجازه از

7. DBIR Snapshot: Intellectual Property Theft 8. Encryption 9. Patent

دارنده‌ی حق یا لایسنس‌گیرنده به نقض اختراع اقدام کند. معمولا مخترع از حق انحصاری ساخت، فروش، استفاده و بهره‌برداری از اختراع برای مدت معین و در قلمرو سرزمینی کشور اعطاکننده‌ی حق اختراع برخوردار است، بنابراین دریافت حق اختراع در یک کشور به معنای داشتن آن حق در دیگر کشورها نیست. این در حالی است که سیستم‌های رایانش ابری ممکن است فراتر از مرزهای بین‌المللی گسترش یابند و در چند کشور واقع شده باشند. طبیعت چندحوزه‌ای رایانش ابری[10] پیچیدگی‌هایی را بر سر راه دارندگان پتنت یا لایسنس‌گیرندگانی قرار می‌دهد که قصد اقامه‌ی دعوا بر ضد ناقضان حق اختراع خود را دارند.

برای مثال اگر مخترعی سیستم پردازشی را اختراع کند و آن را در یک کشور ـمثلا آلمانـ به ثبت برساند و شرکت ارائه‌دهنده‌ی خدمات ابری بدون کسب اجازه از مخترع، سیستم پردازش او را در کشوری دیگر ـمثلا ترکیهـ استفاده کند، احتمالا مخترع نمی‌تواند دعوای نقض حق اختراع خود را در کشوری که در آن نقض صورت گرفته است (ترکیه) طرح کند و باید به راه‌های دیگر همچون مسئولیت مدنی متوسل شود.

علاوه‌براین، پیش‌بینی اینکه چه نوع فعالیت‌هایی به‌طور حتم ناقض حق اختراع تلقی می‌شود نیز دشوار خواهد شد. مثلا اگر فناوری خاصی در کانادا پتنت بگیرد، اما سرویس رایانش ابری رقیب از زیرساخت استفاده کند و تمام یا بخشی از پردازش داده‌های خود را در خارج از کانادا انجام دهد، در این صورت پتنت کانادایی نقض نشده است.

• کپی‌رایت:

حجم زیادی از داده‌ها که در ابر ذخیره شده‌اند، تحت حمایت کپی‌رایت قرار می‌گیرند. این داده‌ها شامل فیلم‌ها، متن‌ها، عکس‌ها، بازی‌ها و برنامه‌های کامپیوتری است. مطابق قانون کپی‌رایت، کسی که اثری را پدید می‌آورد، از حق کپی رایت برخوردار می‌شود و می‌تواند از اثر خود هر طور که صلاح می‌داند استفاده کرده و از جمله آن را در ابر ذخیره کند. ولی تکثیر آن اثر برای هر شخص دیگر به‌طورکلی ممنوع است حتی در ابر.

نکته‌ی دیگر آن است که رایانش ابری متضمن ذخیره‌ی داده در ابر است و ماهیت خاص و ویژه‌ی ابر، تحلیل نقض کپی‌رایت را پیچیده می‌کند، زیرا قوانین کپی‌رایت از حوزه‌ای قضایی به حوزه‌ی قضایی دیگر متفاوت است. عملی که در یک کشور نقض کپی‌رایت تلقی می‌شود، ممکن است در کشور دیگر نقض این قانون نباشد. بنابراین، وقتی داده در محل‌های مختلف ذخیره نباشد مشخص نیست که کپی‌رایت در کدام حوزه نقض شده است.

> **وقتی داده در محل‌های مختلف ذخیره نباشد مشخص نیست که کپی‌رایت در کدام حوزه نقض شده است.**

مسئله‌ی دیگر مربوط به کپی‌رایت این است که آیا ارائه‌دهندگان خدمات ذخیره‌ی ابر می‌توانند برای نقض کپی‌رایت مسئول شناخته شوند یا خیر؟ فرض کنید کاربری محتوای ناقض کپی‌رایت را در ابر بارگذاری کند؛ مثلا موسیقی یا فیلمی را تکثیر کرده و در ابر ذخیره کند. سؤال اینجاست که چه کسی مسئول نقض است. بدیهی است که کسی که عمل تکثیر را انجام داده (در اینجا کاربر)، در وهله‌ی اول مسئول است. اما آیا می‌توان ارائه‌دهنده‌ی خدمات ابری را نیز مسئول دانست؟ رویکرد کشورها در این مورد متفاوت است. برای مثال در انگلستان بر اساس بند ۲ ماده ۱۶ قانون «کپی‌رایت، طرح و پتنت» نه تنها اجازه‌دهنده‌ی عمل نقض را مسئول می‌داند، بلکه ارائه‌دهنده خدمات را نیز مسئول

10. Multi-Jurisdictional Nature of Cloud Computing

که کاربران نگران آن هستند. این موضوع همانند سکه دو رو دارد. یک روی سکه مربوط به ارائه دهنده سرویس ابر است و روی دیگر مربوط به کاربران سرویس رایانش ابری. کاربر پیش از بارگذاری داده‌های محرمانه در ابر، باید توجه کند که ارائه‌دهنده‌ی سرویس ذخیره‌ی ابر، چه نوع تکلیفی درباره‌ی محرمانگی در قبال او دارد. ارائه‌دهنده خدمات رایانش ابری نیز باید این مورد را در نظر داشته باشد که طبق قوانین داخلی کشورشان آیا کاربر اصولا می‌تواند تمامی داده‌های خود را در محیط ابر قرار بدهد؟

به صورت کلی، یک کاربر -شخص حقیقی- مشکلی با اشتراک‌گذاری اطلاعات شخصی خود با ارائه‌دهنده‌ی خدمات ابری ندارد. اما سازمان‌ها ممکن است نگران داده‌های تحت مالکیت خود باشند. در برخی سیستم‌های حقوقی ممکن است قوانین و مقررات اختصاصی برای صنایع و کسب و کارها موجود باشد که اشتراک‌گذاری داده‌ها را به طور کلی ممنوع یا محدود کند. برای مثال، در آمریکا قانون امکان انتقال بیمه سلامت و مسئولیت بیمه‌گران حوزه سلامت[11]، محدودیت‌هایی را برای شرکت‌های مراقبت بهداشتی در خصوص به اشتراک‌گذاری سوابق پزشکی افراد وضع کرده است. همچنین بانک مرکزی هند، دستورالعمل‌هایی را برای بانک‌های این کشور وضع کرده است تا هنگام برون‌سپاری خدمات مالی خود به اشخاص ثالث، از اصول خاصی پیروی کنند.

۳. نکات لازم در قراردادهای رایانش ابری

رایانش ابری از جمله موضوع‌های پیچیده و جدیدی است که هنوز قانونی به‌طور خاص و مفصل بدان نپرداخته است. این امر نه تنها در ایران بلکه در اکثر نظام‌های حقوقی کشورهای دیگر نیز وجود دارد. بنابراین در شرایط کنونی که در این زمینه خلأ قانونی وجود دارد، انعقاد قراردادهای رایانش ابری اهمیتی دوچندان می‌یابد. طرفین قرارداد رایانش ابری باید حتی‌الامکان مسائل و اختلافاتی که ممکن است در آینده بروز یابند را در نظر گرفته و متناسب با آن، راهکارهای لازم را در قرارداد تصریح کنند. این امر میسر نیست مگر در صورتی که مشاوران حقوقی و مذاکره‌کنندگان

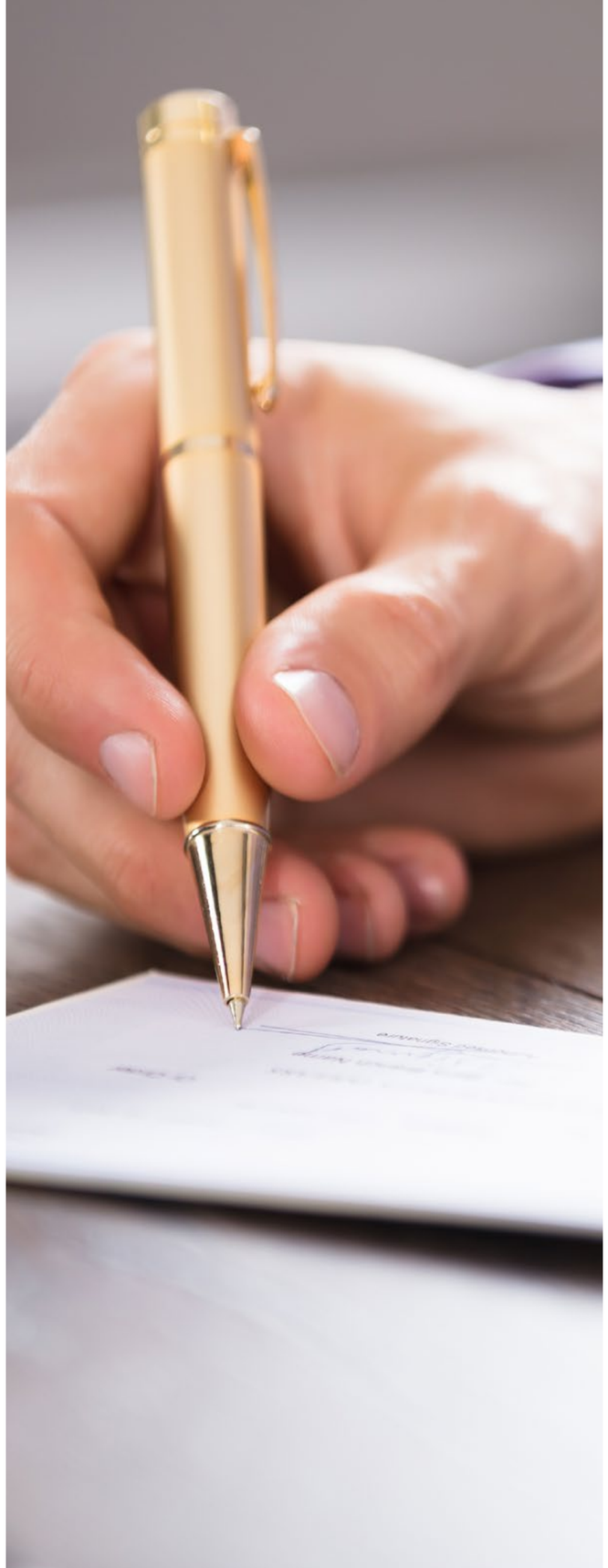
۱۱. قانون امکان انتقال بیمه سلامت و مسئولیت بیمه‌گران حوزه سلامت: طبق این قانون بیمه‌گذار می‌تواند با حفظ امتیازات و اعتباراتی که نزد بیمه‌گر اول کسب کرده است، بیمه‌گر خود را تغییر دهد.

دانسته است. چون اجازه‌ی انجام تکثیر را داده است. اما به نظر می‌رسد که صرف ارائه‌ی خدمات ابری به معنای اعطای اجازه به کاربر برای نقض کپی‌رایت نیست. باید بررسی کرد که آیا ارائه‌دهنده اقدامی برای جلوگیری از نقض کپی‌رایت به عمل آورده است یا خیر. مثلا به کاربران در مورد بارگذاری محتوای ناقض کپی‌رایت هشدار داده است، یا تجهیزاتی که ارائه کرده، تا چه حد در ارتکاب نقض مؤثر بوده است.

رویه‌ی قضایی کانادا این‌گونه حکم داده است که طبق قانون کپی‌رایت کانادا، ارائه‌دهنده‌ی خدمت ابری که واسطه‌ی ارتباط به‌شمار می‌رود و فقط کانالی را برای مبادله‌ی اطلاعات بین دیگران فراهم می‌کند، از مسئولیت مبراست. لیکن بحث بر سر این مسئله همچنان ادامه دارد که آیا عنوان «ارائه‌دهندگان ذخیره‌ی ابری» لزوما با تعریف یک واسط صرف مطابقت دارد یا خیر. بنابراین، در حال حاضر مشخص نیست ارائه‌دهندگان خدمات ابری در کانادا در چه محدوده‌ای از مسئولیت نقض کپی‌رایت نسبت به اطلاعاتی که برای کاربرانشان ذخیره کرده‌اند، مبرا می‌شوند.

• اطلاعات محرمانه و اسرار تجاری:

در محیط ابری، بحث حریم خصوصی و محرمانگی داده‌ها از اهمیت بسزایی برخوردار است. چگونگی حمایت از اطلاعات شخصی و محرمانه مانند اسرار تجاری از موضوعاتی است



قرارداد نسبت به محیط ابری اطلاعات کافی داشته و تمامی جوانب را در نظر بگیرند.

برخی از مهم‌ترین نکاتی که باید در انعقاد قرارداد رایانش ابری بدان توجه شود بدین شرح است:

• مالکیت داده‌ها:

باید توجه داشت که رابطه‌ی مشتری و شرکت ارائه‌دهنده، بر اساس «امانت» شکل گرفته است؛ به‌عبارت‌دیگر، **مشتری مالک داده‌هاست** و آن‌ها را برای ذخیره‌سازی و پردازش نزد ارائه‌دهنده به امانت می‌گذارد، بنابراین انتقال مالکیتی صورت نگرفته و مالکیت مشتری بر داده‌ها همچنان پابرجاست. ارائه‌دهنده امانت‌دار داده‌های مشتریان است و علاوه‌بر انجام تعهدات خود مبنی بر ذخیره‌سازی و پردازش داده‌ها، مسئولیت حفاظت از داده‌های مشتریان را نیز بر عهده دارد.

ولیکن برای پیش‌گیری از هرگونه سوءاستفاده‌ی بعدی بهتر آن است که در قرارداد منعقدشده بین مشتری و ارائه‌دهنده، مالکیت مشتری بر داده‌ها مطرح شود. همچنین باید در قرارداد تصریح شود که ارائه‌دهنده پس از خاتمه‌ی قرارداد، رونوشتی از تمامی اطلاعات مشتری را به او بازگردانده و تمامی اطلاعات موجود نزد خود را از بین ببرد.

• حفاظت از داده‌ها از جانب شرکت ارائه‌دهنده‌ی خدمات

اشاره شد که شرکت ارائه‌دهنده امانتدار داده‌های مشتریان است. از آنجا که مفهوم امانت با حفاظت و نگهداری همراه است بنابراین شرکت وظیفه دارد تمامی اقدامات لازم برای حفاظت از داده‌ها را به عمل آورد. تدابیر فنی همچون رمزگذاری داده‌ها از جمله‌ی این اقدامات حفاظتی است.

باید توجه داشت که چنانچه شرکت ارائه‌دهنده، کوتاهی کند و به موجب این قصور، اختلالی در داده‌ها ایجاد شده یا داده‌ها از بین بروند، مسئول جبران خسارت خواهد بود؛ اما اگر قصور نداشته باشد و تمامی اقدامات حفاظتی لازم را به عمل آورده باشد، مسئولیتی متوجه او نیست.

11. Health Insurance Portability and Accountability Act (HIPAA)

• اقدامات حفاظتی از جانب مشتری

نباید اتخاذ تدابیر حفاظتی را تنها محدود به ارائه‌دهنده دانست. مشتری نیز می‌تواند با درج قیودی در قرارداد، امکان نظارت بر داده‌ها را برای خود فراهم کند. یکی از مواردی که می‌توان بدین منظور در قرارداد درج کرد رمزگذاری داده‌ها[12] است. پیش‌تر اشاره شد که رمزگذاری نقش مؤثری در حفاظت از داده‌ها دارد و آن را از دسترس هکرها و مجرمان سایبری مصون می‌دارد، اما نقش دیگر رمزگذاری را باید در فراهم‌کردن نظارت مشتری نسبت به داده‌ها دانست. مشتری با در اختیار داشتن رمز داده‌های خود قادر به رمزگشایی[13] و نظارت بر داده‌های خود است. مشتری با انتخاب ناظر یا ناظرانی که دانش و تخصص لازم را درباره رایانش ابری به خصوص امنیت داده‌ها در محیط ابری دارند، می‌تواند گام موثری در تامین امنیت داده‌های متعلق به خود بردارد.

دیگر قیود نظارتی که می‌توان در قرارداد درج کرد عبارتند از: حق نظارت بر رویه‌های امنیتی[14] و نظارت بر مراکز داده[15]، مقرره‌ای مبنی بر آگاه‌سازی فوری مشتری در صورت وقوع هرگونه نقض ترتیبات امنیتی و مقرره‌ای درباره‌ی اعطای اجازه به ناظری از خارج شرکت برای ارزیابی کنترل‌ها و رویه‌های ذخیره، مدیریت و انتقال داده‌ها.

همچنین در صورتی که مشتری خواهان حفاظت ارائه‌دهنده از اطلاعات بخصوصی باشد و ارائه‌دهنده نیز مسئولیت حفاظت از آن اطلاعات را تضمین کند، در این صورت نمی‌تواند از تعهد خود شانه خالی کند و در قبال امنیت آن داده‌ها مسئول است.

• بیمه‌ی داده‌های مشتریان

پوشش بیمه‌ای داده‌های مشتریان راهی مناسب برای جبران خسارت مشتری در صورت از بین‌رفتن داده‌ها یا ایجاد نقص در آن‌هاست. البته باید توجه داشت که ممکن است برخی شرکت‌های بیمه برای بیمه‌کردن اطلاعات در فضای ابری محدودیت‌هایی داشته باشند، بنابراین طرفین باید سیاست‌های شرکت بیمه را به خوبی مطالعه کرده و با آگاهی کامل اطلاعات را بیمه کنند.

12. Data Encryption 13. Decryption 14. Security Procedures
15. Data Centers

• انعقاد قرارداد سطح خدمت

قرارداد سطح خدمت[16]، بخشی از قرارداد ارائه‌ی خدمات یا قراردادی تکمیلی در کنار قرارداد اصلی ارائه‌ی خدمات است که بین مشتری و ارائه‌دهنده‌ی خدمت منعقد شده و مسائل مربوط به کیفیت خدمات ارائه‌شده و موضوعات تأثیرگذار بر آن را پوشش می‌دهد. برای مثال درصورتی‌که در ارائه‌ی خدمات تأخیری ایجاد شود یا دسترسی به شبکه برای ساعاتی در روز قطع شود، به کیفیت خدمت خدشه وارد شده و طبق ضمانت اجرایی که در قرارداد تعیین شده است، عمل خواهد شد.

• قراردادهای امانت (Escrow)

اگرچه رایانش ابری مزایای متعددی دارد، اما از خطرهای احتمالی آن نیز نباید چشم‌پوشی کرد. ممکن است ارائه‌دهنده، نسخه‌های پشتیبان حاوی داده‌های حساس مشتریان را گم کند یا اینکه اختلالی در سیستم‌های شرکت به وجود آمده و داده‌ها از بین بروند. در مواردی که داده‌ها بسیار حساس بوده و در صورت آسیب به داده‌ها، تولید دوباره آن‌ها امکان‌پذیر نیست. پیشنهاد می‌شود که مشتری اطلاعات خود را در نزد شخص ثالثی به غیر از شرکت ارائه‌دهنده به امانت بگذارد که اصطلاحا به آن قرارداد امانت «اسکرو» می‌گویند. در اینجا نیز باید حتما در قرارداد قید شود که پس از خاتمه‌ی قرارداد، تمام رونوشت‌های اطلاعات به مشتری بازگردانده شده و آنچه نزد شرکت قرار دارد نیز کاملا از سیستم پاک شود.

• ارائه‌ی اطلاعات مشتریان به اداره‌ی مالیات و سایر سازمان‌های دولتی در صورت لزوم

با توجه به اینکه بسیاری از داده‌هایی که در اختیار شرکت‌های ارائه‌دهنده‌ی خدمات رایانش ابری قرار می‌گیرد جنبه‌ی مالی دارد، این سؤال مطرح است که آیا این شرکت‌ها باید در صورت درخواست سازمان امور مالیاتی یا دیگر سازمان‌های دولتی، اطلاعات مشتریان را در اختیار این سازمان قرار دهند یا اینکه باید این اقدام را به ارائه‌ی حکم قضایی از جانب سازمان امور مالیاتی منوط کنند؟

16. Service Level Agreement (SLA)

به عنوان مثال در نظام حقوقی ایران طبق مقررات مالیاتی، در مواردی که مدارک و اسناد حاکی از تحصیل درآمد نزد اشخاص ثالث باشد، اشخاص ثالث مکلفند با مراجعه و مطالبه‌ی ادارات امور مالیاتی، دفاتر و همچنین اصل و یا رونوشت اسناد مربوط و هرگونه اطلاعات مربوط به درآمد مؤدی یا مشخصات او را ارائه دهند.

در مورد اطلاعاتی که در فرآیند رایانش ابری ذخیره و نگهداری می‌شود، مسئله مهم این است که نمی‌توان آن را از مصادیق مواردی دانست که مدارک و مستندات نزد شخص ثالث باشد. چون در این موارد شرکت ارائه‌دهنده خدمات صرفا محلی برای ذخیره اطلاعات در اختیار مشتری قرار می‌دهد و هیچ مدارکی حاکی از تحصیل درآمد نزد شرکت وجود ندارد به خصوص اینکه دسترسی شرکت به اطلاعات مشتری نیز همیشه با محدودیت‌هایی مواجه است. ویژگی امانت بودن اطلاعاتی که مشتری در ابر ذخیره می‌کند شالوده‌ی قرارداد و خدمات رایانش ابری است. بنابراین، هرگونه ارائه اطلاعات مشتری به اداره مالیات و سایر سازمان‌های دولتی منوط به ارائه‌ی دستور قضایی از مراجع صالح است.

این موضوع نه تنها در خاک یک کشور بلکه ممکن است در مواردی که ارائه‌دهنده‌ی خدمات ابری در خارج از کشور مستقر است و مالک اطلاعات تبعه‌ی کشور دیگر است نیز اجرا شود. برای مثال اگر دادگاهی آمریکایی که مراکز داده‌ها در آن قرار دارد مجوز ضبط اطلاعات و داده‌های سازمان کشوری دیگر صادر کند، خدمات‌دهنده‌ی آمریکایی موظف به ارائه آن اطلاعات خواهد بود. موضوعی که معمولا در بخش Terms of Use وب‌گاه‌های رایانش ابری به آن اشاره می‌شود.

در پایان این نکته شایان توجه است که هر قدر هم که در تهیه‌ی قراردادها دقت به خرج داده شود اما همواره این احتمال وجود دارد که خطری غیرقابل پیش‌بینی داده‌های مشتریان را تهدید کند. ازاین‌رو لازم است پیش از استفاده از خدمات رایانش ابری، توان مدیریتی شرکت‌های ارائه‌دهنده و سابقه‌ی آن‌ها در رایانش ابری ارزیابی شود.

مزایای استفاده از خدمات ابری

گفت‌وگو با فرید فولادی

معاون توسعه‌ی بازار همکاران سیستم

در این بخش گفت‌وگویی با فرید فولادی، معاون توسعه‌ی بازار همکاران سیستم، انجام شده است. در این گفتگو به مزایای استفاده از رایانش ابری و تجربیات حاصل از ارائه راهکار نرم‌افزاری رایانش ابری شرکت همکاران سیستم در بازار ایران با عنوان راهکاران ابری اشاره شده است. جزئیات این گفت‌وگو در ادامه تشریح شده است:

- **«رایانش ابری» تا چه حد فراگیر می‌شود؟**

در واقع فراگیر شده است، اما بعضی بخش‌ها و نرم‌افزارها با تاخیر از این مدل استفاده می‌کنند. ضمن این‌که هنوز بسیاری از ارائه کننده‌ها، زیرساخت را خودشان ایجاد می‌کنند، یک دیتاسنتر درست می‌کنند و سرویس را به مردم ارائه می‌دهند. این مدل فعلا مرسوم است خصوصا در کشور ما که عرضه‌کننده‌های بزرگ زیرساخت‌های «رایانش ابری» نیستند. به‌تدریج در دنیا این روش در حال تغییر است و سرویس‌دهندگان در لایه‌های مختلف زیرساخت، پلتفرم و نرم‌افزار خدمت ارائه می‌کنند. به همین دلیل دیگر نیاز نیست همه‌ی سرویس‌دهندگان برای خودشان دیتاسنتر مستقل درست کنند. برای کاربر نهایی هم مهم نیست زیرساخت توسط چه ارگانی تامین می‌شود و فقط مهم است که سرویس درستی دریافت کنند.

- **آیا این تجمیع سرویس‌ها و خدمات و به‌طور کلی اطلاعات، نکته‌ی مثبتی است؟**

به نظرم به‌تدریج بازار به یک تعادل در این زمینه می‌رسد. یعنی نه تا این حد فضا پراکنده می‌شود که همه‌ی سرویس‌دهنده‌ها دیتاسنتر خودشان را داشته باشند و نه آن‌قدر متمرکز که فقط یک شرکت باقی بماند. زمانی‌که سرویس‌دهندگان می‌خواهند از زیرساخت یک شرکت دیگر استفاده کنند، لحظه‌ی بسیار مهمی است و آن‌جا عوامل بسیاری بررسی می‌شود تا مشخص شود که آیا این دیتاسنتر به حد کافی قابل اعتماد است که شما حاضر بشوید سرویسی را که قرار است به کاربران ارائه کنید روی آن قرار دهید و خیال‌تان از بابت همه‌ی مسائل آن راحت باشد یا خیر؟

- **چرا جهانی که مملو از راه‌حل‌ها و ابزارهای تکنولوژی بود به‌سوی «رایانش ابری» رفت و به بیان دیگر «رایانش ابری» چه ارزش جدیدی را ایجاد می‌کند که مورد توجه قرار گرفته است؟**

به نظر من «رایانش ابری» برخلاف بسیاری از سرویس‌ها که استفاده از آن‌ها با شرکت‌های بزرگ شروع می‌شود، از مردم شروع شد؛ یعنی کاربر نهایی زودتر از سازمان‌ها جذب این سرویس شدند. یکی از دلایل این موضوع سادگی استفاده از آن بود و کاربر درگیر پیچیدگی نرم‌افزاری نمی‌شود. شاید برای شما هم پیش آمده باشد، قبلا کسانی‌که به نرم‌افزار تسلط داشتند همیشه باید پاسخ‌گوی دوستان و آشنایانی می‌بودند که برای نصب و راه‌اندازی یک نرم‌افزار دچار مشکل می‌شدند و مداوما نیاز داشتند از فرد متخصصی کمک بگیرند تا آن نرم‌افزار را عملیاتی کند، درحالی‌که در فضای «رایانش ابری» این معضل به‌طور کامل حل شده و همه‌ی درگیری‌های نصب و راه‌اندازی از کاربر به سرویس‌دهنده منتقل شده است. این سادگی و کاربرد ساده‌ی «رایانش ابری» باعث شد تا به‌سرعت توسعه پیدا کند و امروزه تقریبا کسی نیست که از آن استفاده نکند.

سازمان‌ها اما در برابر «رایانش ابری» در ابتدا مقاومت کردند. اولین و مهم‌ترین دلیل این مقاومت هم این بود که به چه سرویس‌دهنده‌ای اعتماد کنند؟ و سوالات فراوان دیگر مانند این‌که اگر سرویس قطع شود چه اتفاقی خواهد افتاد؟ یا در صورت استفاده از «رایانش ابری» چه اتفاقی برای دیتای من می‌افتد و چقدر امنیت آن تامین می‌شود؟ و یا با تجهیزاتی که تا امروز برای راه‌اندازی و نگهداری آن هزینه کرده‌ایم چه کنیم؟ موضوع دیگر این بود که به نرم‌افزارهای خریداری شده احساس مالکیت داشتند و این موضوع برای آن‌ها مهم بود. اما این مشکلات به‌تدریج حل شد. مشکل اول حل شد به این دلیل که سرویس‌های بسیار خوبی وارد بازار شد و سرعت و دسترسی به اینترنت هم به وضعیت پذیرفتنی رسید. موضوع بعدی محرمانگی داده‌هاست که تا حدود زیادی حل شده است، اما در دنیا هنوز این موضوع باز است و ابهاماتی در آن وجود دارد. این ابهامات در همه‌ی دنیا به‌سرعت در حال شفاف‌سازی و رفع‌شدن است و برای همه‌ی مسائل آن قانون‌های خوبی اجرایی شده و می‌شود.

• همان‌طور که شما هم اشاره کردید، یک بحث دیگر بحث دسترسی غیرمجاز به اطلاعات است، در این زمینه چه نگرانی‌هایی وجود دارد و چه راه‌حل‌هایی در صورت انتخاب فناوری «رایانش ابری» پیش روی مشتریان این سرویس‌ها قرار خواهد گرفت؟

سرویس‌دهنده‌های نرم‌افزار بر بستر «رایانش ابری»، در این زمینه بسیار حساس هستند؛ چرا که امانت‌دار مشتریان خود هستند و سرویس‌دهنده‌های معتبر، تمامی الزامات و مراقبت‌های لازم را فراهم می‌کنند، مراقبت‌هایی که معمولا مشتریان، به‌دلیل نیاز به تخصص و هزینه‌های بالا، نمی‌توانند تامین کنند. برای نمونه، ما در همکاران سیستم چند لایه امنیتی ایجاد کرده‌ایم و خود کارشناسان شرکت هم با محدودیت‌های بسیار و با اطلاع مشتری به دیتای او دسترسی دارند. اما دو واقعیت دیگر را هم در نظر بگیرید، اول این‌که امنیت فقط دسترسی غیرمجاز نیست و مشتریان معمولا

موضوعات بسیار مهم‌تری را رعایت نمی‌کنند که یک سرویس‌دهنده با وسواس به آن‌ها توجه می‌کند، مانند تهیه‌ی نسخ پشتیبان، دردسترس بودن همیشگی، امکان بازیافت سریع اطلاعات و مانند آن.

باید توجه کرد دسترسی فقط یک وجه از امنیت است، آیا سازمان‌ها به این موضوع فکر می‌کنند که اگر هارد سرور آن‌ها بسوزد یا بر اثر یک اتفاق خراب شود چه پیامدی دارد؟ اگر شبکه‌ی آن سازمان دچار مشکل شود و دسترسی کارمندان به سرور قطع شود، چه اتفاقی می‌افتد؟ اگر فردی در خود سازمان به اطلاعات دسترسی پیدا کند و آن را خراب کند، چه می‌شود؟

در مجموع دیتا زمانی که بر روی سرورهای سرویس‌دهنده است امنیت بیشتری دارد تا زمانی‌که پیش خود مشتری قرار دارد. در نمونه‌ی کوچک‌تر، شاید بتوان گفت همه‌ی ما تجربه‌ی نگهداری عکس‌های یادگاری را در هارد اکسترنال داشته‌ایم، چه‌قدر احتمال دارد این هارد از دست شما بیافتد؟ چه‌قدر احتمال دارد آن را گم کنید یا این‌که سرقت شود. اما زمانی‌که از سرویس ابری مثل گوگل فوتو استفاده می‌کنید، همه‌ی عکس‌های شما دردسترس شماست و به‌خوبی از آن مراقبت می‌شود. اگر سازمان‌ها به امنیت فکر می‌کنند، قطعا امنیت اطلاعات آن‌ها در کلاد بیش‌تر است.

دوم این‌که عمده‌ی مشکلات امنیتی و حتی دسترسی‌های غیرمجاز در درون سازمان‌ها رخ می‌دهد چرا که از رویه‌ها و مدل‌های استاندارد تبعیت نمی‌شود.

بسیاری از مشتریان ما نگران دیتای کسب‌وکار خود هستند و می‌ترسند که این اطلاعات افشا شود، درحالی‌که به‌راحتی گزارش‌های مالی خود را بارها برای افراد مرتبط ایمیل می‌کنند. دلیل این‌که نگران این موضوع نیستند شاید این است که دقت لازم را ندارند. اما باید به این نکته هم توجه کرد که دنیا درحال حرکت به‌سمتی است که امنیت تبادل اطلاعات در آن بسیار حیاتی است و این وظیفه‌ی مهندسانی است که در این زمینه تخصص دارند و باید این امنیت را برای تبادل اطلاعات تامین کنند.

عمده‌ی مشکلات امنیتی و حتی دسترسی‌های غیرمجاز در درون سازمان‌ها رخ می‌دهد چرا که از رویه‌ها و مدل‌های استاندارد تبعیت نمی‌شود.

زیرساخت‌های فنی رایانش ابری، بستری امن برای داده‌های مشتری

از مهمترین مزایای استفاده از فضاهای ابری برای پردازش اطلاعات، واسپاری بخش عمده موضوعات زیرساختی به شرکت دیگری است که می‌تواند هزینه‌های سربار سازمان‌ها را در حد چشم‌گیری کاهش دهد. اما یکی از نگرانی‌های تمام افراد و یا شرکت‌هایی که قصد دارند برای اولین بار از زیرساخت‌های ابری، به عنوان فضایی برای پردازش داده‌های خویش استفاده کنند، چگونگی حفظ امنیت داده‌هایشان، لو رفتن اطلاعات به رقبا، احتمال بررسی محتوای داده‌های ایشان در سیستم‌های اطلاعاتی ابری و موضوعات مشابه است.

در ادامه، سعی بر آن است تا این موضوع که زیرساخت‌های فنی رایانش ابری، چگونه می‌توانند به حفظ مالکیت فکری مشتریان، کمک نموده و ضامن امنیت داده‌های ایشان باشند را از جنبه‌های مختلف مورد بررسی قرار دهیم.

۱. امنیت داده‌ها

امنیت داده‌های مشتریان، از دو حیث قابل بررسی است؛ اول، امنیت داده‌ها به معنای ایجاد امنیت و پیشگیری از بروز رخدادی است که باعث از دست رفتن داده‌ها[17] شود و ایجاد مکانیزم‌هایی برای بازیابی داده‌ها و عملیاتی کردن سیستم‌ها در صورت بروز مشکل از دست رفتن دیتا[18]، دوم، امنیت داده‌ها به معنای پیشگیری از دسترسی پیدا کردن به اطلاعات توسط هکرها، رقبا، نرم‌افزارهای مخرب و حتی دسترسی پیدا کردن افراد بیرون از شرکت ارائه‌دهنده خدمات ابری[19] به اطلاعات مشتری، که هر دوی این موارد بسیار مهم و قابل بررسی است.

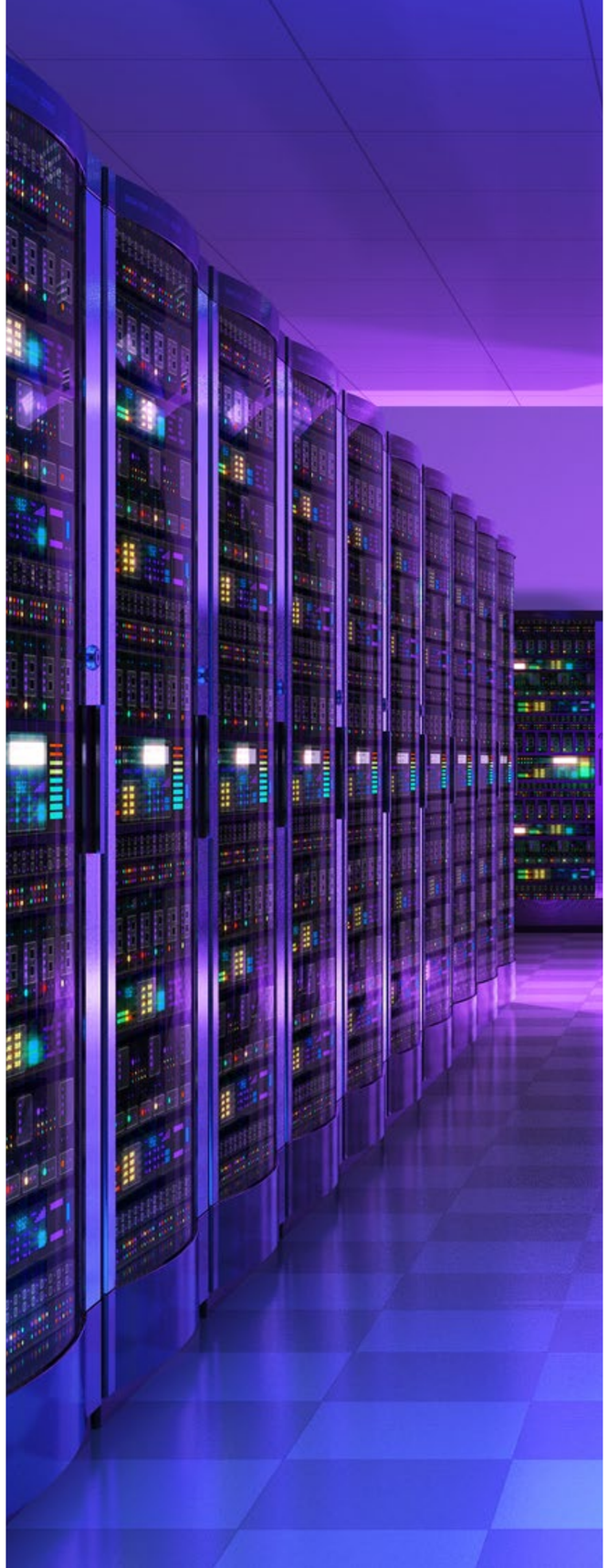
• امنیت در نگهداری داده‌ها

یکی از وظایف مهم شرکت‌هایی که خدمات ابری آنها شامل پردازش داده‌های مشتریان می‌شود، مانند شرکت‌های ارائه‌دهنده خدمات ابری (SaaS)، تعریف صحیح و مشخص از نحوه نگهداری و تهیه کپی پشتیبان[20] از داده‌های مشتری و همچنین ارائه ضمانت مشخص مدت زمان، برای حداکثر میزان اطلاعاتی است که در صورت بروز مشکلات اساسی ممکن است از دست برود. اصلاحا به این عمل PRO [21] می‌گویند که معمولا برحسب ساعت، یا در بدترین حالت، برحسب روز است.

شرکت‌های ارائه دهنده برای رسیدن به سطح بالایی از RPO و امکان ارائه ضمانت در این مورد، لازم است زیرساخت‌های متفاوتی تهیه کنند. به عنوان مثال، این شرکت‌ها لازم است قبل از هر چیز در طراحی زیرساخت‌های خود، انواع متفاوتی از افزونگی‌ها[22] را در نظر گرفته باشند که تا جای ممکن در صورت بروز مشکل در بخشی از زیرساخت‌ها، مانند سرورها، دیسک‌ها و موارد دیگر، بخش افزونه معادل، مسئولیت بخش دارای مشکل را بر عهده بگیرد و عملا مشکلی بر ای کل سیستم و بالطبع مشتری ایجاد نشود. افزونگی در سیستم‌ها و ساختار IT، به مواردی گفته می‌شود که برای یک کار خاص، دو یا چند نمونه مشابه وجود دارد که کار یکسان انجام می‌دهند و در موارد لزوم می‌توانند نقش یکدیگر را ایفا کنند. به عنوان مثال، اگر یک سیستم به ۵۰۰ وات انرژی احتیاج داشته باشد، در طراحی‌ها از دو منبع تغذیه ۵۰۰ واتی استفاده می‌شود که در صورت بروز مشکل برای یکی، دومی، نقش آن را ایفا کند و سیستم در کل دچار مشکل نشود.

در عین حال زیرساخت‌های این شرکت‌ها باید همیشه برای شرایط غیرقابل اجتناب نیز طراحی مشخصی داشته باشند. شرایطی که در آن افزونگی‌ها نیز ممکن است دچار

17. Data Loss 18. Disaster Recovery 19. 3rd party 20. Backup
21. Recovery Point Objective 22. Redundancy



مشکل شوند، شرایطی که سرورهای متفاوت با هم از دسترس خارج شوند و حوادث طبیعی مانند سیل، زلزله، آتش‌سوزی‌ها و دیگر بلایای طبیعی که ممکن است یک ناحیه از کشور را تحت تاثیر قرار دهند یا زیرساخت‌های موجود منطقه را به کلی از بین ببرند. برای چنین شرایطی لازم است طراحی‌های مشخصی مانند انتقال کپی‌های پشتیبان به مناطق جغرافیایی دیگر در بازه‌های زمانی مشخص، ایجاد ساختارهای توزیع‌شده [23] و موارد دیگر نیز در طراحی ساختار رایانش ابری در نظر گرفته شده باشد.

ساختارهای توزیع‌شده، به این مفهوم است که ساختار سرورها، مراکز داده‌ها و.. در چند محل جغرافیایی وجود دارد و این ساختارها با هم در ارتباط هستند. داده‌ها نیز در هر چند محل به صورت هم‌زمان وجود دارد تا در صورت بروز مشکل، از دیگر محل‌ها استفاده و مشکلی برای سیستم‌ها ایجاد نشود که در واقع نوعی افزونگی در سطوح بالاتر است.

آیا همه شرکت‌های ارائه‌دهنده خدمات ابری، این شرایط را در نظر می‌گیرند؟

طبعا خیر، هر شرکتی بسته به هزینه و منفعت موجود برای خود و مشتریان بالقوه، ممکن است همه یا بخشی از موارد ذکر شده را در نظر گرفته باشد یا حتی هیچ یک از موارد را در نظر نگرفته باشد. هرچند شرکت‌های معتبر ارائه دهنده راهکارهای نرم‌افزاری ابری، الزاما می‌بایست تمام موارد فوق را در طراحی خویش مدنظر گرفته باشند.

مهم‌ترین و بهترین راه مطمئن شدن از این موضوع که تا چه حد موارد فوق در طراحی زیرساخت ابری نظر گرفته شده است، بررسی وجود عبارت «تعهد نگهداری داده‌های مشتریان» و مشخص بودن میزان RPO در قرارداد است.

• امنیت در دسترسی به داده‌ها

اطلاعاتی که در نرم‌افزارهای اطلاعاتی ذخیره می‌شوند حاوی جزئیات بسیار مهمی از کسب و کار است. به عنوان نمونه، اطلاعاتی چون فرمول‌های تولید، اطلاعات تأمین‌کنندگان و مشتریان، اطلاعات حقوق و دستمزد کارکنان و سایر موارد مشابه فقط بخشی از میلیون‌ها اطلاعاتی هستند که در

23. Distributed

چنین سیستم‌هایی مورد پردازش قرار می‌گیرند. افشای این اطلاعات به هر شکلی می‌تواند در کنار نقض مالکیت فکری داده‌ها، عواقب جبران ناپذیری برای سازمان‌ها به همراه داشته باشد.

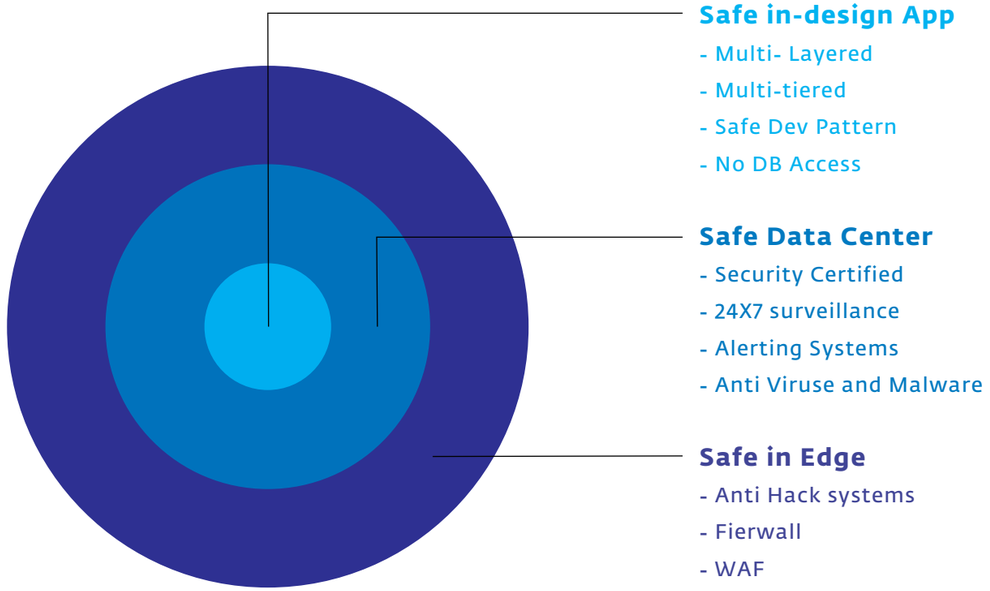
لذا یکی از مهمترین وظایف شرکت‌های ارائه‌دهنده خدمات ابری، اطمینان از به‌کارگیری راهکارهایی است که بتواند ضمانت لازم برای جلوگیری از افشای اطلاعات و داده‌های مشتریان را فراهم کند. چنین راهکارهایی شامل موارد متعدد و متنوعی می‌شود که بخشی از آن فنی و قسمتی نیز مربوط به نحوه سیاست‌گذاری‌های انجام‌شده در شرکت است. به عنوان مثال، اینکه چه بخش‌ها یا واحدهایی از یک سازمان ارائه‌دهنده خدمات نرم‌افزاری ابری، امکان دسترسی به اطلاعات مشتریان را دارند به سیاست‌گذاری کلی شرکت مربوط است که اجرای سیاست مزبور از طریق راهکارهای فنی پوشش داده می‌شود. اما اینکه مکانیسم‌هایی برای جلوگیری از نفوذ هکرها به سیستم‌ها وجود داشته باشد، به هیچ عنوان به نحوه سیاست‌گذاری شرکت مذکور، مربوط نبوده و جزو الزامات هر ساختار ابری محسوب می‌شود.

در حالت مطلوب، در شرکت‌های معتبر ارائه‌دهنده خدمات نرم‌افزاری، ایجاد حداقل دسترسی به داده‌های مشتریان در سازمان، می‌بایست جزو سیاست‌های اصلی سازمان باشد و مطلوب آن است که کمترین سطح دسترسی مستقیم به داده‌های مشتریان، وجود داشته باشد (یا در بهترین حالت هیچ دسترسی نباید وجود داشته باشد). همچنین، شرکت‌های معتبر به طور پیش فرض، در قراردادهای خود موارد مرتبط با تفاهم‌نامه عدم افشا یا NDA [24] را نیز در مورد داده‌های مشتریان مدنظر قرار می‌دهند.

اما در مورد موارد فنی، موضوعات پیچیده‌تری نیز وجود دارد و اطلاعات در سیستم‌های ابری لازم است در لایه‌های متعددی امن شوند.

برای روشن‌تر شدن موضوع، در ادامه مثالی از زیرساخت یک سیستم Software as a Service، که می‌توان گفت تقریبا بالاترین پیچیدگی امنیتی برای پیاده‌سازی را در بین انواع مختلف Cloud باید داشته باشد بیان می‌شود.

همانطور که در تصویر شماتیک زیر مشاهده می‌کنید،



24. Non-disclosure agreement

یک نرم‌افزار SaaS در هسته اصلی خود یک نرم‌افزار دارد که در نهایت قرار است مشتری با این نرم‌افزار کار کند. این نرم‌افزار از لحاظ طراحی، باید نرم‌افزاری امن باشد. به این معنی که تیم تولید این نرم‌افزار، باید آن را به نحوی طراحی کرده باشند تا امکان نفوذ به سیستم در صورت حمله هکرها، نرم‌افزارهای مخرب و موارد مشابه در آن بر اساس موارد شناخته شده وجود نداشته باشد.

البته باید دقت داشت که چنین طراحی‌های امنی، هزینه‌های تولید نرم‌افزار را به صورت چشم‌گیری افزایش می‌دهند. به این دلیل که برای چنین مدل‌های طراحی حداقل‌هایی مانند طراحی چند لایه[25] نرم‌افزار، ساختارهای امن تولید نرم‌افزارهای تحت‌وب[26] و موارد دیگر وجود دارد که جزو حداقل‌های چنین طراحی‌هایی است. این مدل های طراحی و همچنین موارد مهم دیگری که به عنوان راهنماهای امن‌سازی نرم‌افزار، در مراجع معتبری چون OWASP[27]،معرفی می‌شود، برای پیاده‌سازی نیاز به برنامه‌نویسان خبره و کارشناسان فنی خبره و زمان زیاد برای طراحی دارد. به همین دلیل همه شرکت‌های نرم‌افزاری ارائه‌دهنده خدمات ابری، لزوما چنین هزینه‌ای را متقبل‌نمی‌شوند.

حتی در برخی شرکت‌های نرم‌افزاری ارائه دهنده، ممکن است با نرم‌افزارهای شبه ابری[28] مواجه شویم که به طور معمول نرم‌افزارهای عادی غیر وب هستند. این نرم‌افزارها به وسیله برخی نرم‌افزارهای مجازی‌سازی محیط کار[29] به صورت مشابه وب و ابری ارائه می‌شوند و استفاده از چنین نرم‌افزارهایی به عنوان راهکار ابری به طور کلی توصیه نمی‌شود.

در مرحله بعدی، مرکز داده‌ای که داده‌های نرم‌افزار را نگهداری می‌کند قرار گرفته، که لازم است موارد مختلف امنیتی در طراحی خود مرکز داده و فرآیندهای آن رعایت شده باشد. این موارد شامل تمام موارد امنیتی در ارتباطات شبکه داخلی، دسترسی افراد، فرآیندهای بررسی خطاها[30]، نگهداری و کنترل‌های روتین و همچنین تعمیرات اساسی[31]و دیگر موارد است که هر کدام الزامات و نکات امنیتی متعددی را مانند مکانیسم‌های پایش، سیستم‌های اعلام هشدار، فرآیندهای داخلی مشخص برای عملیات جاری و موارد مهم دیگری را نیاز دارد.

> **در شرکت‌های معتبر ارائه‌دهنده خدمات نرم‌افزاری، ایجاد حداقل دسترسی به داده‌های مشتریان در سازمان، می‌بایست جزو سیاست‌های اصلی سازمان باشد و مطلوب آن است که کمترین سطح دسترسی مستقیم به داده‌های مشتریان، وجود داشته باشد .**

در مرحله بعدی لازم است ارتباطات بین مرکز داده‌ها با مشتریان و ایستگاه‌های کاری آن‌ها امن شود. با توجه به اینکه این بخش تنها نقطه ارتباط زیرساخت‌های داخلی سیستم ابری با بیرون است، نیاز به مراقبت ویژه‌ای دارد. برای نمونه، برای جلوگیری از نفوذ هکرها نیاز به انواع فایروال‌های خاص و هوشمند از جمله WAF[32] وجود دارد که به طور معمول دستگاه‌هایی گران قیمت هستند که لازم است به صورت دقیق و متناسب با نرم‌افزار تنظیم شده و در طراحی شبکه سیستم‌های ابری استفاده شود. یا برای پیشگیری از لو رفتن اطلاعات حساس در ارتباطات با مدل‌های هک Man in the Middle یا Sniffing، نیاز به رمزگذاری[33] اطلاعات خط ارتباطی با استفاده از SSL[34] و استفاده از پروتکل HTTPS[35] در ارتباط وجود دارد.

اما به عنوان یک مشتری چطور می‌توانیم از همه این موارد امنیتی مطمئن شویم؟ قاعدتا هیچ شرکتی امکان بازدید یا بازگو کردن جزئیات طراحی شبکه خود را به دلایل امنیتی، به مشتریان نخواهد داد.

25. Multi-Tiered, Multi-layered 26. Safe Development Patterns 27. Open Web Application Security Project 28. Faux Cloud 29. Desktop Virtualization
30. Troubleshooting 31. Overhaul 32. Web Application Firewall 33. Encryption 34. Secure Sockets Layer 35. Hypertext Transfer Protocol Secure

در واقع نیازی هم به این کار وجود ندارد. تنها نکته مهم، بررسی وجود گواهینامه‌های معتبر امنیتی برای زیرساخت و نرم‌افزار ارائه شده است. از جمله این گواهینامه‌ها، می‌توان به ISO 27001 یا ISMS اشاره کرد، که در کنار بررسی نکات امنیتی در زیرساخت‌ها و فرآیندها، اطمینان حاصل می‌کند که زیرساخت‌ها و فرآیندهای موجود در سازمان ارائه دهنده، محرمانگی، در دسترس بودن و صحت داده‌های مشتری را نیز حفظ می‌کنند یا به عبارت دیگر بخشی مهمی از مالکیت معنوی مرتبط با داده‌های مشتریان با وجود چنین گواهینامه‌هایی تضمین خواهد شد.

۲. الزامات و استانداردهای لازم به تناسب محل استفاده

یک نکته مهم که در استفاده از سیستم‌های ابری باید به آن توجه شود، محل جغرافیایی استفاده از نرم‌افزار است که ممکن است الزامات امنیتی، یا استانداردهای لازم سیستم‌ها را تحت تاثیر قرار دهد.

به عنوان مثال، وجود گواهینامه افتا [۳۶] برای برخی نرم‌افزارها در ایران و در شرکت‌های مرتبط با دولت الزامی است، یا از ۲۵ ام ماه می سال ۲۰۱۸، رعایت استاندارد GDPR [۳۷] برای تمام نرم‌افزارهایی که در کشورهای عضو اتحادیه اروپا استفاده می‌شوند الزامی شده است و حتی عدم رعایت این قانون در اروپا می‌تواند جریمه‌های بسیار سنگین نقدی برای سازمان‌ها در برداشته باشد.

این موارد جزو موضوعاتی است که بسته به نوع استفاده سازمان‌ها و شرکت‌ها از سیستم‌های ابری، لازم است در نظر گرفته شود.

شرکت‌های ارائه دهنده نیز، بر اساس نیازمندی‌ها و الزامات مشخص شده، لازم است تغییراتی در نرم‌افزار یا زیرساخت‌های خود انجام دهند، تا چنین استانداردهایی را پوشش دهند. هر چند عملا این موضوع که یک شرکت نرم‌افزاری بتواند تمامی استانداردهای موجود در تمامی حوزه‌ها را پوشش دهد، امکان پذیر نیست.

جمع‌بندی

به طور کلی، در صورتی که نیازمندی‌ها و استانداردهای لازم چه از لحاظ نگهداری داده‌ها و چه موضوعات امنیت و پایش اطلاعات [۳۸] برای یک کسب‌وکار و سازمان مشخص باشد، استفاده از سیستم‌های رایانش ابری که این استانداردها را پوشش دهد، هم از دید هزینه و هزینه‌های سربار و هم از منظر هزینه‌های لازم برای پوشش استانداردها و الزامات کسب‌وکار، می‌تواند تاثیر شگرفی بر کسب‌وکارها، خصوصا کسب‌وکارهای نوپا، داشته باشد. اگر این موارد رعایت شوند ابر به مراتب امن‌تر از حالت‌هایی است که داده‌ها توسط خود مشتریان پردازش شود.

36. امنیت فضای تبادل اطلاعات
37. General Data Protection Regulation
38. Audit

درباره روز جهانی مالکیت فکری و رویکرد سال ۲۰۱۹

در سال ۲۰۰۰ میلادی دولت‌های عضو وایپو تصمیم گرفتند روز ۲۶ آوریل-روزی که کنوانسیون وایپو در سال ۱۹۷۰ لازم‌الاجرا شد -را با هدف افزایش آگاهی عمومی درباره‌ی مالکیت فکری «روز جهانی مالکیت فکری» تعیین کنند. وایپو هر سال نام ویژه‌ای را برای این روز تعیین می‌کند که هر کدام از آن‌ها، مبنای فعالیت‌های وایپو در آن سال قرار می‌گیرد. در سال ۲۰۱۹ روز جهانی مالکیت فکری با عنوان رسیدن به طلا: مالکیت فکری و ورزش نام‌گذاری شده است.

۲۰۱۸- زنان در نوآوری و خلاقیت

۲۰۱۷- اختراع: بهبود زندگی

۲۰۱۶- خلاقیت دیجیتال: فرهنگ دوباره تصویر شده

۲۰۱۵- بیدارشو، برخیز برای موسیقی

۲۰۱۴- فیلم‌ها: یک علاقمندی جهانی

۲۰۱۳- خلاقیت: نسل بعدی

۲۰۱۲- مخترعان رویا پرداز

۲۰۱۱- طراحی آینده

۲۰۱۰- نوآوری: ارتباط دهنده‌ی دنیا

۲۰۰۹- ارتقاء نوآوری به عنوان کلید آینده مطمئن

۲۰۰۸- جشن نوآوری و احترام به مالکیت فکری

۲۰۰۷- ارتباط بین مالکیت فکری و خلاقیت

۲۰۰۶- مالکیت فکری با یک ایده شروع می‌شود

۲۰۰۵- فکر کن، تصور کن و خلق کن

۲۰۰۴- اهمیت مالکیت فکری برای اقتصاد و توسعه فرهنگی و اجتماعی

۲۰۰۳- مالکیت فکری را کسب وکار خود کنید

۲۰۰۲- تشویق خلاقیت

۲۰۰۱- همین امروز آینده را خلق کنید

۲۰۱۹- رسیدن به طلا: مالکیت فکری و ورزش

منابع

1. Patrick J. Laycock, Cloud computing: A brief overview of intellectual property issues "in the cloud", November 16, 2011, available at:
<http://www.smart-biggar.ca/en/articles_detail.cfm?news_id=535>, last visited: 18/02/2019

2. Asaf, Cidon, protecting intellectual property in the cloud, available at: <https://www.wipo.int/wipo_magazine/en/2015/03/article_0004.html>, last visited: 02/03/2019

3. The legal aspects of cloud computing under the copyright law, available at: https://www.wbs-law.de/eng/it-law/the-legal-aspects-of-cloud-computing-under-copyright-law-45886 , last visited: 08/03/2019/

۴ - مذاکرات قراردادهای سطح خدمت، مندرج در:
https://motamem.org/مذاکره-توافق-نامه-سطح-خدمات/

۵ - صادقی نشاط، امیر، قرارداد سه جانبه Escrow در نرم‌افزار، دانشکده حقوق و علوم سیاسی دانشگاه تهران، تابستان ۱۳۸۵، شماره ۷۲، مندرج در:
http://ensani.ir/file/download/article/20120419185549-8024-332.pdf