کاربرد فناوری زنجیره‌های بلوکی در تأمین امنیت اطلاعات الکترونیک قضایی

محمد جواد شاکری [۱]
آیدا مخترع [۲*]
بهنام رستگاری [۳]

تاریخ دریافت مقاله: ۱۴۰۳/۰۱/۰۲ **تاریخ پذیرش نهایی:** ۱۴۰۳/۰۶/۰۵

چکیده

زنجیره بلوکی (بلاک چین) یکی فناوری جدید در زمینه رایانش ایمن است. این فناوری می‌تواند دنیای دیجیتال را متحول کند و با استفاده از خصوصیت «تفاهم توزیع یافته» برای هر فعالیت آنلاین قدیمی یا فعلی، فعالیت را به نحوی اجرا نماید که داده‌های دیجیتالی در آینده نیز قابل شناسایی و اعتماد باشند. این امر بدون در خطر افتادن حریم خصوصی و امنیت دارایی‌های درگیر انجام می‌گیرد و با توجه به پیشرفت‌هایی که فناوری زنجیره‌های بلوکی دارد و هر روز در حال توسعه است، بیشتر سازمان‌ها در تلاش هستند تا بتوانند از طریق مرتبط کردن سرویس‌های خود با این تکنولوژی خدمات بهتری را ارائه کنند. قوه قضاییه از جمله سازمان‌هایی است که درصدد است با بهره‌گیری از فناوری زنجیره‌های بلوکی، عملکرد خود را بهبود بخشد. بنابراین پژوهش حاضر با هدف به نمایش گذاشتن کاربرد فناوری زنجیره‌های بلوکی در ارائه خدمات قضایی و نقش این فناوری در حفاظت از داده‌های قضایی به رشته تحریر درآمده است. یافته‌های پژوهش حاکی از آن است دولت و قوه قضاییه از فناوری زنجیره‌های بلوکی برای پوشاندن شکاف‌های تکنولوژیک بهره می‌برند و با استفاده از فناوری‌های نوین که برای رشد و پایداری بسیار مهم بوده جهت حفاظت از داده‌های قضایی بهره می‌گیرند. و اگر نوعی سیستم ثبت اطلاعات در دستگاه‌های قضایی ایجاد گردد که بر پایه فناوری بلاک چین کار کند، این سیستم قرار است میان تمام اعضای شبکه که به آن متصل هستند به اشتراک گذاشته شود و اطلاعات آن از طریق یک بلاک به بلاک دیگر منتقل شود. این اطلاعات تنها به صورت رمزنگاری شده قابل انتقال هستند.

واژگان کلیدی: زنجیره‌های بلوکی، خدمات الکترونیک قضایی، امنیت اطلاعات.

مقدمه

[۱] دانشجوی کارشناسی ارشد گروه حقوق خصوصی، مؤسسه آموزش عالی آپادانا، شیراز، ایران. shakerimohamad567@yahoo.com
[۲] استادیار و عضو هیئت علمی مؤسسه آموزش عالی آپادانا، شیراز، ایران. (نویسنده مسئول): dr.mokhtare@apadana.ac.ir
[۳] استادیار دانشکده حقوق و علوم سیاسی دانشگاه شیراز، شیراز، ایران. behnam.rastegari.law@gmail.com

الکترونیکی شدن دادرسی‌ها[1] روندی بوده که در یک دهه گذشته به جهت مزایای آن و سرعت بخشیدن به رسیدگی‌ها در کشورها مورد استفاده قرار گرفته است. لکن رفته رفته سیستم‌های قضایی برای امنیت بیشتر به دنبال ارائه خدمات قضایی در بستر بلاک چین[2] می‌باشند. (شهبازی نیا و دیگران، ۱۲۲:۱۳۹۶)

فناوری «زنجیره‌های بلوکی» یا «بلاکچین» پدیده‌ای نوظهور در جهان است که می‌تواند تحولات قابل توجهی در عرصه‌های مختلف مالی و غیر مالی اعم از سیستم قضایی ایجاد نماید. زنجیره بلوکی یک فناوری دفتر کل توزیع شده می‌باشد که پتانسیل نوآورانه بالایی در همه زمینه‌های خدمات مالی و غیر مالی دارد. این داده‌ها در یک شبکه از کامپیوترهای توزیع شده به اشتراک گذارده می‌شود. در واقع زنجیره بلوکی شبکه‌ای از کامپیوترهاست که از طریق اینترنت به هم متصل بوده و کاربران این کامپیوترها قادر هستند داده‌ها، هویت و دارایی را بدون واسطه تبادل نمایند. (یوسفی و دیگران، ۱۴۰۰: ۵) بلاک‌چین که زنجیره‌ای از بلوک‌ها می‌باشد در واقع یک بانک اطلاعاتی توزیع شده یا غیر متمرکز است. فناوری زنجیره بلوکی بدون نیاز به یک شخص ثالث قابل اعتماد یا واسط، اطمینان و شفافیت بالایی ارائه می‌کند و مزایایی از جمله کاهش هزینه و زمان و افزایش امنیت را می‌تواند به دنبال داشته باشد. بدین ترتیب که در مقام مقایسه می‌توان گفت فناوری بلاک چین همانند اینترنت پایدار و قدرتمند است، اما برخلاف اینترنت وب۲[3] (اینترنت امروزی) بلاک‌های یکسان از اطلاعات را در شبکه خود نگهداری می‌کند.[4] به همین دلیل بلاک

[1] منظور از دادرسی الکترونیکی آن است که جهت طرح دعوی و فرآیند دادرسی از ابزارها و روش‌های الکترونیکی اطلاعاتی و ارتباطی استفاده گردد.

[2] block chain

[3] شبکه جهانی وب که به طور ساده به عنوان اینترنت یا وب نیز شناخته می‌شود، از زمانی که برای اولین بار با نام Web1 به جهان معرفی شد، به شدت تغییر کرده است. همانطور که فناوری‌ها بهبود می‌یابند و تقاضای کاربران تکامل می‌یابد، جای تعجب نیست که وب نیز بر این اساس تغییر کرده باشد. Web1 برای مصرف محتوا و تعامل ساده استفاده می‌شود. وب ۲ که تا حدی با رونق تلفن‌های هوشمند و دسترسی به اینترنت موبایل شکل گرفته است، کاربران را قادر می‌سازد تا محتوای خود را ایجاد کنند. اکنون، مفهوم جدیدی از یک وب آینده به نام وب ۳ ظهور کرده است. این اینترنت آینده به دنبال فناوری‌هایی مانند بلاک چین، هوش مصنوعی (AI) و واقعیت افزوده (AR) است. مهم تر از همه یک وب ۳ (Web3) ایده‌آل باید مزایایی مانند مالکیت داده ها و محرمانه بودن را ارائه دهد. وب ۳ به عنوان یک نسخه بهبود یافته از وب ۲ معرفی می‌شود.

[4] به زبان ساده بلاک چین یک اپلیکیشن غیرمتمرکز است که مسئولیت آنچه در بلاک شما قرار دارد، بر عهده خود شما است. برای مثال اگر کلید کیف پول بلاک چین خود را گم کنید، درواقع راه دسترسی به پول خود را برای ابد و همیشه از دست داده‌اید. در واقع بلاک چین نوع خاصی از پایگاه داده است که اطلاعات در آن در قالب دفتر کل توزیع‌شده، غیرمتمرکز و اشتراکی ذخیره می‌شود. شما مالک داده‌های خود در یک بلاک چین هستید و اینکه شخص دیگری برنامه را توسعه داده است، به این معنی نیست که آن شخص می‌تواند داده‌های شما را ببیند؛ البته دقیقا به همین دلیل هم در صورت گم کردن رمز عبورتان، نمی‌تواند در بازیابی کردن آن به شما کمکی کند. در مثالی دیگر، در سیستم

چین را هیچ موجودیت منفردی نمی‌تواند کنترل کند و فاقد نقطه شکست واحد است. با ذخیره سازی داده‌ها در شبکه بلاک چین، ریسک‌های مرتبط با ذخیره سازی متمرکز داده‌ها را از بین می‌برد. شبکه‌های بلاک چین فاقد آسیب پذیری نقاط متمرکز است که هکرهای کامپیوتری بتوانند از آن بهره ببرند و این در حالی است که اینترنت امروزی مشکلات امنیتی خاصی دارد که برای همگان مشخص شده است و غالباً از نام کاربری و گذرواژه برای دسترسی به داده‌های آنلاین خود استفاده می‌کنیم. بلاک چین از فناوری رمز نگاری برای بهبود امنیت استفاده می‌کند. بلاک چین با توزیع گسترده داده‌ها و اطلاعات، ستون فقراتی را برای اینترنت جدید، یعنی وب ۳[۱] ایجاد کرد. (بامبارا[۲] و آلن[۳]، ۱۲:۱۳۹۷) گرچه فناوری بلاک چین با گسترش شهرت رمز پول‌ها به ویژه بیت کوین در رسانه‌ها و در میان مردم، بر سر زبان‌ها افتاده است. لذا بسیاری فکر می‌کنند بلاک‌چین‌ها تنها در مورد رمز پول‌ها نظیر بیت کوین سخن می‌گویند، اما این فناوری بسیار فراتر از این تصور هستند. فناوری بلاک‌چین تقریباً در تمامی حوزه‌های خصوصی و دولتی کاربرد دارد (کهن هوش نژاد و پاک‌ذات، ۶:۱۳۹۷) و در حال حاضر، رشد انفجاری در صنایع مالی، سلامت، بیمه و حکمرانی و دولت و قضا داشته است و تازه این اول راه است. بدین ترتیب که علاوه بر کشورهای پیشرو در این زمینه همچون کانادا، مکزیک، ایالات متحده، آرژانتین، اتحادیه اروپا کشورهای دیگری مانند استرالیا، چین، ژاپن، امارات، مالت، سوئیس، ایالات متحده، استونی، بریتانیا، سنگاپور و ... بهره‌برداری از این فناوری در بخش‌های مختلف را شروع کرده‌اند.

فناوری بلاک چین در زمینه امور قضایی و چالش‌های انفورماتیک آن در راستای ایجاد امنیت مضاعف نیز راه حل‌هایی دارد که در پژوهش حاضر نیز برآنیم نقش فناوری زنجیره‌های بلوکی در ارائه خدمات قضایی را مورد بررسی قرار داده و سودمندی حاصل از این اثرگذاری من جمله افزایش امنیت داده‌ها و حفظ حریم خصوصی شهروندان را مورد تحلیل قرار دهیم چرا که این فناوری

بانک‌داری سنتی، مدیران بانک‌ها می‌توانند موجودی حساب بانکی شما و میزان برداشت‌های شما را ببینند و خب از سوی دیگر هم می‌توانند در صورت فراموشی رمز عبور، به شما کمک کنند. در مقابل، اگر یک کیف پول ارز دیجیتال اتریوم، را در نظر بگیرید، بنیان‌گذار آن ارز دیجیتال، نمی‌داند شما در کیف پول خود چقدر موجودی دارید.

[۱] وب ۳ که به عنوان **وب** باهوش هم شناخته می‌شود، علاوه بر ایجاد تعامل و ارتباط بین افراد و سایت ها، امکان ارتباط بین نرم افزار ها رو هم بوجود آورده است. البته این فناوری همچنان در حال تکامل است ولی هیچ ایده ای در مورد شکل نهایی این نسل از اینترنت وجود ندارد.

[۲] Bambara

[۳] Alan

می‌تواند همانند اینترنت که انقلابی عظیم در عرصه‌های مختلف بشری از قرن بیستم تا کنون ایجاد کرده است، تحولات عظیم و آثار شگرفی را به وجود بیاورد.

الف) ادبیات پژوهش

۱- مفهوم و تاریخچه زنجیره‌های بلوکی[۱]

در ادامه به بررسی مفهوم شناسی به صورت فنی و تاریخچه فناوری زنجیره‌های بلوکی خواهیم پرداخت.

۱-۱- مفهوم زنجیره‌های بلوکی

زنجیره‌های بلوکی یا همان بلاک‌چین یک ساختمان داده می‌باشد که امکان ایجاد یک دفترکل عمومی از داده‌ها و به اشتراک گذاشتن آن‌ها میان‌شبکه‌ای از طرف‌های مستقل را فراهم می‌نماید. بلاک‌چین انواع بسیاری دارد که عبارتند از:

- بلاک‌چین‌های عمومی؛ همانند بیت‌کوین که شبکه‌های بزرگ توزیع شده می‌باشند و از شیوه یک توکن بومی اجرا می‌گردند. این‌ها برای هر کسی و در هر سطحی که مشارکت دارد، باز می‌باشد و دارای کد منبع‌باز برای جامعه‌ای می‌باشد که از آن‌ها نگهداری می‌کند. (کهن هوش نژاد و پاک ذات، ۱۳۹۹: ۹۶)
- بلاک‌چین‌های دارای مجوز؛ نظیر ریپل، نقش‌هایی را که اشخاص قادر خواهند بود داخل شبکه اجرا نمایند کنترل می‌کنند. این‌ها کماکان سیستم‌های بزرگ و توزیع شده‌ای می‌باشند که از یک توکی سومی استفاده می‌کنند که اصلی آن‌ها ممکن است منبع‌باز باشد یا نباشد.
- بلاک‌چین‌های خصوصی؛ کوچک‌تر نوع بوده و از ترکی استفاده نمی‌نمایند. عضویت در این نوع بلاک‌چین‌ها بسیار کنترل شده می‌باشد. این نوع بلاک‌چین‌ها موردعلاقه کرسیوم هایی است که دارای اعضای مورد اعتماد بوده و اطلاعات محرمانه مبادله می‌نمایند.

همه انواع بلاک‌چین‌ها از رمزنگاری استفاده می‌کنند که به مشارکت‌کنندگان با هر شبکه معین دیگری اجازه خواهند داد دفتر عمومی کل را بدون نیاز به مقام رسمی به شکل مطمئن و ایمن

[۱] Block chain

شده برای اعمال قوانین مدیریت نمایند. مهم‌ترین و قدرتمندترین جنبه زنجیره‌های بلوکی، حذف مقام رسمی مرکزی از ساختار پایگاه‌داده‌ها می‌باشد.

بلاک‌چین‌ها؛ سوابق و تاریخچه تراکنش‌ها را به صورت دائمی ثبت می‌کنند. اما در واقع هیچ‌چیزی دائمی نیست. در فضای بلاک‌چین‌ها این بدان معناست که بخش بزرگی از جامعه بلاک‌چین همگی توافق دارند که اطلاعات را تغییر داده لکن به‌اندازه کافی انگیزه دارند که داده‌ها را تغییر ندهند.

هنگامی که داده‌ای در بلاک‌چین ثبت می‌شود تغییر یا حذف آن بسیار دشوار است. هنگامی که کسی بخواهد سابقه‌ای را به بلاک‌چین اضافه کند. که به آن تراکنش یا مدخل می‌گویند، کاربرانی که در آن شبکه کنترل تأیید را در اختیار دارند، تراکنش پیشنهادی را ممیزی می‌کنند. اینجاست که کار کمی پیچیده می‌شود زیرا هر بلاک‌چینی قلق نسبتاً خاص خود را در چگونگی انجام کار و اینکه چه کسی می‌تواند تراکنش را تأیید کند، دارد. (کهن هوش نژاد و پاک ذات، ۱۳۹۹: ۹۷)

۱-۲- تاریخچه زنجیره‌های بلوکی

شخص یا گروهی به نام «ساتوشی ناکاماتو»[۱] در سال ۲۰۰۸ مقاله‌ای تحت عنوان «بیت کوین: سیستم پول نقد الکترونیکی همتا به همتا»[۲] منتشر نمود. این مقاله، معرفی نسخه‌ای از پول نقد الکترونیکی را معرفی می‌نمود که قادر به انجام پرداخت‌های آنلاین به صورت مستقیم و بدون نیاز به عبور از سیستم یک مؤسسه مالی از یک شخص به شخص دیگر بود. اولین اشاره به این مفهوم بیت کوین بود. امروزه هم برچسبی با عنوان «ارز رمز پایه» برای توصیف تمام رسانه‌های ارزی و شبکه‌ها است که تراکنش‌های ایمن را با استفاده از رمز نگاری، ایجاد می‌نماید و در مقابل سامانه‌هایی واقع می‌شوند که در آن سامانه‌ها تراکنش‌ها از طریق یک نهاد مرکزی مطمئن کانال دهی می‌گردند. مقصود نویسنده مقاله اولیه بر این بود که مورد شناسایی قرار نگیرد و تا به امروز تفاهمی در هویت «ساتوشی ناکاماتو» انجام نشده است. یک برنامه با منبع آزاد چند ماه بعد به منظور اجرایی نمودن این پروتکل جدید منتشر گردید که برای شروع با بهره‌گیری از قالب مولد[۳]

[۱] Satoshi Nakamoto

[۲] Peer to peer

[۳] Genesis Block

۵۰ سکه تعریف می‌نمود. همه مجاز بودند این برنامه منبع آزاد را نصب نمایند و بخشی از شبکه همتا به همتای بیت‌کوین شوند که این سیر صعودی محبوبیت از همان زمان شروع گردید.

در سال ۲۰۰۸ به تاریخ ۱۸ آگوست دامنه با نام «bitcoin.org» ثبت شد؛ و به تاریخ ۳۱ اکتبر مقاله طرح بیتکوین منتشر شد؛ و به تاریخ ۹ نوامبر پروژه بیتکوین در sourceforge.net ثبت شد.

در سال ۲۰۰۹ نیز به تاریخ ۳ ژانویه قالب مولد در ساعت 18:15:05 GMT ایجاد شد؛ و به تاریخ ۹ ژانویه نسخه ۰/۱ منتشر شد؛ و به تاریخ ۱۲ ژانویه اولین تراکنش بیتکوین در قالب ۱۷۰ از «ساتوشی» به «هال فینی» روی داد.

از آن تاریخ به بعد محبوبیت بیت‌کوین هیچگاه متوقف نشده و کاهش نیافته است و اینک فناوری زیرساختی زنجیره بلوکی طیف جدیدی از برنامه‌های مالی را پوشش می‌دهد. (رجبی و فریور، ۱۳۹۶: ۵-۴)

۲- مفهوم حریم خصوصی اطلاعاتی

حریم خصوصی قلمرویی از زندگی معنوی و مادی بشر است که انتظار می‌رود جز با رضایت او هیچ شخص دیگری در آن ورود ننماید و یا آن را مورد پایش قرار ندهد. شاید در یک عبارت بسیار ساده و کوتاه بشود یک مفهوم کامل از حریم خصوصی بیان نمود. ساده ترین و کوتاه ترین تعریف «حق تنها و با خود بودن» به کار برده شده است. (صادقی، ۲:۱۳۸۶) بنابراین حریم خصوصی یکی از با ارزش ترین حقوق اساسی اشخاص یک جامعه می‌باشد که اشخاص با امنیت کامل در آن به زندگی خصوصی خود می‌پردازند و هیچ گونه دغدغه و نگرانی از بابت تجاوز و تعدی به حریم خصوصی امن شخصی خویش و افشای اطلاعات شخصی نداشته باشند. به نحوی که امروزه یکی از بنیادی‌ترین اصول حقوق بشر رعایت حریم خصوصی اشخاص می‌باشد.

«حریم خصوصی در قلب آزادی و در کشوری مدرن وجود دارد. حریم خصوصی بر اساس آزادی عمل جسمی و اخلاقی بشر و اساساً جهت رفاه و آسایش شخص بنا نهاده شده است. صرفاً به این دلیل شایسته حمایت اساسی می‌باشد، اما در عین حال، ماهیتی بنیادی در خصوص نظم عمومی دارد. محدودیت‌هایی که بر حکومت به منظور اجتناب از تجسس در زندگی شهروندان اعمال می‌گردند به اساس و ماهیت یک دولت دموکراتیک بر می‌گردد».(استیون هیک و دیگران، ۲۸۳:۱۳۸۶)

علاوه بر اشتراک اصل حمایت از حریم خصوصی اشخاص، حدود و ابعاد حریم خصوصی به فرهنگ و زمینه‌های محیطی و اجتماعی بستگی تام دارد. بر این مبنا وضعیت حمایت از حریم خصوصی اشخاص در جهان و در نظام‌های حقوقی مختلف متفاوت می‌باشد.

حریم خصوصی دارای چهار حوزه مختلف اعم از حریم خصوصی اطلاعاتی، حریم خصوصی ارتباطات، حریم خصوصی مکانی یا حریم خصوصی در منازل و اماکن و حریم خصوصی جسمانی؛ می‌باشد، که در اینجا به تعریف حریم خصوصی اطلاعاتی خواهیم پرداخت.

حریم خصوصی اطلاعاتی تحت عنوان «حمایت داده» در برخی از نظام‌های حقوقی بررسی می‌شود و عبارت از قواعد حاکم بر نحوه پردازش اطلاعات و داده‌های مربوط به افراد است. پردازش داده هر گونه فعل و انفعالاتی را شامل می‌شود که در خصوص یک داده اتفاق می‌افتد. تحصیل، ساماندهی، نگهداری، ذخیره، جایگزینی، اصلاح، افشاء، تغییر، انتشار و انتقال داده از قبیل این فعل و انفعالات هستند. بر اساس اصول حاکم بر حمایت از داده‌ها تمامی اطلاعات شخصی همانند اطلاعات مالی اشخاص، اطلاعات پزشکی آن‌ها، اطلاعات دولتی و نظایر آن می‌بایست تحت قواعد مربوط به حمایت داده پردازش گردند و هر گونه تخطی از قواعد مزبور به منزله نقض حریم اطلاعاتی افراد تلقی می‌گردد. این نوع حریم یک نهاد حقوقی جدیدی می‌باشد که به موازات توسعه ارتباطات الکترونیکی به ویژه در حوزه شبکه‌های رایانه‌ای و اینترنت بروز شده است. (صادقی، ۳:۱۳۸۶)

ب) مخاطرات ارائه خدمات الکترونیک قضایی در نقض حریم خصوصی شهروندان

آن چه شهروندان را در راستای ارائه خدمات الکترونیک قضایی دچار چالش خواهد نمود، به سرقت رفتن داده‌های مندرج در شبکه خدمات الکترونیک قضایی می‌باشد که در ادامه به توضیح آن می‌پردازیم.

۱- فقدان امنیت سایبری

بحث امنیت در دنیای تبادل داده‌ها، جایگاه و اهمیت ویژه‌ای دارد، امنیت به قدری حیاتی و مهم می‌باشد که در تدوین قانون آیین دادرسی الکترونیکی، قانونگذار چند ماده را به مقوله امنیت اختصاص داده و برای نقض کنندگان آن نیز مجازات‌هایی تعیین نموده است. مطابق با این موضوع که هم هویت مخاطب یا طرفین به صورت مطمئن قابل شناسایی باشد، و هم حریم خصوصی اشخاص با بهره از رایانه و اینترنت آشفته نشود و در نهایت اینکه ابزارهای موثق و مطمئن که از

گواهی‌های استاندارد شبکه جهانی استفاده می‌نمایند محیط امن سایبرنتیک را برای متداعیین فراهم کند (رضائی‌نژاد و محسنی، ۱۳۹۱:۱۳۲).

مقصود از واژه امنیت، حالتی می‌باشد که از طرفی ممکن است پرونده‌های موجود در اینترنت، مخدوش یا معدوم گردند و از طرف دیگر، امکان دارد مشخصات خصوصی اشخاص برملا و فاش گردد.

بسیاری از گفت و گوها و مدارکی که در جلسات رسیدگی ارائه می‌گردند جنبه محرمانه و سری دارند؛ بدین جهت طرفین انتظار افشای آنان از جانب مقام رسیدگی کننده را ندارد یا این که مقام رسیدگی کننده برای مبادله آن‌ها از ابزارهایی غیرمطمئن بهره بگیرد. هرگاه مدارک و لوایح به صورت الکترونیکی ردوبدل شود این واهمه وجود دارد که شخصی در شبکه نفوذ کند و به آن‌ها دسترسی یابد یا محتوای آنها را تغییر دهد (السان، ۱۳۹۳:۲۰۵).

به چند موضوع در خصوص احتمال مخدوش گردیدن اطلاعات در دادرسی الکترونیکی باید توجه داشت: اولین موضوع در خصوص احتمال وقوع «جعل الکترونیکی» است، یعنی وقتی عنوانی مثل دادرسی الکترونیک را پذیرفته باشیم؛ کم کم ادله الکترونیکی مثل حافظه‌های الکترونیکی یا «CD» که محتواهای اثبات کننده موضوعات کیفری و مدنی را در بر دارند، نیز ظاهر می‌شود. احتمال وقوع جعل در خصوص این ادله نیز، می‌رود، یعنی امکان دارد فیلمی که از تصویر یک سارق است یا اقرار مندرج در آن‌ها؛ ساختگی و غیر واقعی یا تحریف شده باشد. با وجود این شرایط، نیاز هست با استفاده از کارشناسان مربوط و به نحو مقتضی با پدیده جعل الکترونیکی که نتیجه ظهور فرایند دادرسی الکترونیک است، مقابله شود. مخصوصاً برخی اوقات این جعل در مطالبی است که در حین دادرسی ثبت و اظهارشده است، به این معنا که در دادرسی الکترونیک یکی از موضوعاتی که مطرح می‌شود، مقوله پرونده‌های الکترونیک است که مجموع صحبت‌ها و مذاکرات انجام شده در هنگام دادرسی یک جزء آن است. همانگونه که گفته شد این پرونده‌ها نیز قرار گرفته در بستر فضای مجازی می‌باشد. با این تفاسیر امکان دارد اشخاصی با انجام جعل یا «هک الکترونی» آنان را – چه بسا در بردارنده نظریه کارشناس، اقرار و دیگر ادله الکترونیکی می‌باشند – مورد خدشه قرار دهند. در هر صورت به خاطر وجود چنین ایراداتی نمی‌توان، اصل استفاده از فایل‌های الکترونیکی را نادیده گرفت؛ لکن می‌بایست چاره‌ای اندیشیده شود و به نظر می‌رسد بهترین شیوه استفاده از فنّاوری‌هایی می‌باشد که کمتر قابل نفوذ هستند (مهرافشان، ۱۳۹۰:۱۳۸).

۲- نقض حریم خصوصی شهروندان

از دیگر چالش‌های اجرایی دادرسی الکترونیکی و ارائه خدمات قضایی به صورت الکترونیک، می‌توان از امکان نقض حریم خصوصی نام برد که امکان دارد به دنبال امکان دسترسی به پرونده‌های قضایی از طریق کد رهگیری و پیگیری سوابق پرونده قضایی واقع شود. بی‌تردید حق دسترسی به موضوعات دفتر ثبت دعاوی، همه پرونده‌های الکترونیک و نظریات دادگاه، با حق شناخته شده دیگری در تعارض قرار دارد که آن نیز حریم خصوصی است. ابزارها و شیوه‌هایی که به عنوان مایه دادرسی الکترونیکی قلمداد می‌گردند پای دولت به میزانی بیشتر از دولت‌های خودکامه در حریم خصوصی شهروندان باز می‌کند چرا که شیوه‌های الکترونیکی و ابزارها برای امنیت شهروندان و رویارویی با جرم، اینجا خود به عدم امنیت ذهنی و روانی آنان در برابر کنترل شدنشان از سوی دولت مبدل می‌شوند. بدین صورت چون دادرسی الکترونیکی بر پایه دسترسی به اطلاعات و دیده‌بانی الکترونیکی قرار دارد؛ نقطه مقابل رویکرد حقوق بشری می‌باشد. در واقع گاهی فضای اینترنت و ابزارهای الکترونیکی بیشتر از آن که ابزارهای مناسبی برای صیانت از حقوق شهروندان و به‌طور ویژه حقوق متهم استفاده شوند برای قدرت و امنیت دولت مورد استفاده قرار می‌گیرند (مؤذن‌زادگان و روستا، ۱۷۹:۱۳۹۶).

گذشته از موضوع اخیر جهت اعتبار بخشیدن به فرایند تبادل اطلاعات دادرسی به فراخور گستردگی پهنای باند اینترنتی و روزآمد کردن تأمین امنیت شبکه‌های الکترونیکی، قانونگذاران برخی از کشورها ازجمله ایران اقدام به پیش‌بینی سیستم شناسایی هویت اطراف دادرسی با توجه به شماره بایگانی پرونده‌ها، امضای الکترونیکی و ایجاد سیستم کد رهگیری پرونده‌ها نموده‌اند (شهبازی نیا و دیگران، ۱۳۶:۱۳۹۶). در نظام حقوقی ایران با اینکه ماده قانونی به حفظ حریم خصوصی افراد در آیین دادرسی الکترونیکی اختصاص یافته اما هنوز ابهامات زیادی در این مورد وجود دارد؛ ازجمله اینکه ماده ۶۵۸ مقرر می‌دارد: «قوه قضاییه موظف است تمهیدات فنی و قانونی الزم را برای حفظ حریم خصوصی افراد و تأمین امنیت داده‌های شخصی آنان، در چارچوب اقدامات این بخش فراهم آورد» یا ماده ۶۵۹ که مقرر می‌دارد: «به کارگیری سامانه‌های ویدئوکنفرانس و سایر سامانه‌های ارتباطات الکترونیکی، به منظور تحقیق از اصحاب دعوی، اخذ شهادت از شهود یا نظرات کارشناسی در صورتی مجاز است که با احراز هویت، اعتبار اظهارات فرد مورد نظر و ثبت مطمئن سوابق صورت پذیرد» و سرآخر ماده ۶۶۰ نیز مقرر می‌دارد: «چنانچه اشخاصی که داده‌های موضوع این بخش را در اختیار دارند، موجبات نقض حریم خصوصی افراد یا محرمانگی اطلاعات را فراهم آورند یا به طور غیرمجاز آنها را افشا کرده یا در دسترس اشخاص فاقد صلاحیت قرار دهند، به حبس از دو تا پنج سال یا جزای نقدی از بیست تا دویست میلیون ریال و انفصال از

خدمت از دو تا ده سال محکوم خواهند شد».این ماده درباره افشای غیرارادی و قهری یا سرقت داده‌ها سخنی به میان نیاورده است و تکلیف قضیه هنوز مشخص نیست.

همانگونه که تعداد زیادی مأمور و نگهبان برای دادگاه معمولی مورد نیاز است، به همان موازات می‌بایست در دادگاه الکترونیکی مراحل امنیتی اجرا گردد. دادگاه الکترونیکی برای محفوظ ماندن مستندات و تأمین امنیت باید از حالات امنیتی، همچون«پروتکل امنیتی اس.اس.ال»[1] استفاده نماید و بر ضرورت استفاده از یک سیستمِ عاملنفوذ ناپذیر و امن تأکید داشته باشد. گذشته از این‌ها آموزش و افزایش مهارت کاربران موجب می‌گردد به مراتب کار نفوذگران با مشکل مواجه شود، زیرا در سال ۲۰۰۶ مطابق با بررسی‌های شرکت امنیتی سیمانتک تنها استفاده کاربران ناشی بزرگترین هدیه سازمان‌ها به سارقان اطلاعات، بوده است (به‌گذر، ۱۰:۱۴۰۲). به این معنا که عدم امنیت و عدم رعایت موارد ایمن در محیط کاربران از دستبرد غیرکاربران و سارقان این نوع محیط‌ها بوده است.

ج) ایمن سازی اطلاعات شبکه خدمات الکترونیک قضایی

یکی از مسائل جدید در زمینه جرایم و علوم قضایی دیجیتال، آمادگی گروهی برای مقابله با حملات در امنیت شبکه‌های رایانه‌ای در بستر اینترنت همانند شبکه خدمات الکترونیک قضایی است که برای محافظت از داده‌ها و سامانه‌ها و پیشگیری از ایجاد مشکلات امنیتی در بستر شبکه صورت می‌گیرد. از همین رو، امنیت شبکه‌ها همواره مورد توجه کاربران و به ویژه سازمان‌هایی همانند قوه قضاییه که خدمات امنیتی و عمومی ارائه می‌دهند قرار دارد. «حملات امنیتی و رخنه به شبکه‌های رایانه‌ای سازمان‌ها ممکن است داده‌های محرمانه را به خطر انداخته، اعتماد مشتریان را کاهش داده، روابط عمومی را ضعیف ساخته و منجر به اختلال در کارها و تحمیل خسارات مالی شود؛ به علاوه از دست رفتن داده‌های سازمانی، باعث بروز تهدیداتی از قبیل تحریف، باج‌خواهی، سرقت هویت، سرقت فناوری و حتی خطراتی علیه امنیت ملی می‌شود». بنابراین تهدیدات امنیتی موجب شده تا اقداماتی به منظور بالا بردن ضریب امنیتی داده‌های محرمانه و داده‌هایی که توسط ارائه دهندگان خدمات عمومی در ارتباط با خدمات سازمان‌های دولتی یا نیمه دولتی تبادل می‌شود، انجام بگیرد.

[1] SSL: Secure Sockets Layer

منظور از امنیت اطلاعات در بستر اینترنت، مفهوم خاص آن، حفاظت از داده‌ها در برابر افراد غیرمجاز و کنترل کردن سطوح دسترسی کاربران می‌باشد. از این جهت که فناوری‌های وب، زیرساخت‌های نرم‌افزاری پیچیده دارند، با نقض امنیت اطلاعات سایبری نیز مواجه خواهیم بود و وقتی که فناوری‌های وب مختل شود، می‌توانند به عنوان عامل‌های حمله مورد استفاده قرار گیرند. اما امنیت در مفهوم عام آن مسائل متعددی را شامل می‌شود و اهداف گوناگونی همانند تأیید هویت کاربران، کنترل دسترسی، صحت داده‌ها، محرمانگی اطلاعات و غیر قابل انکار بودن ارسال و دریافت اطلاعات را دنبال می‌کند. امنیت اطلاعات در محیط سایبر نیز عبارت است از حفظ منافع افراد یا نهادهای وابسته به اطلاعات، سیستم‌ها و ارتباطات ارائه دهنده اطلاعات در قبال آسیب‌های ناشی از فقدان، از دست رفتن محرمانه بدون انسجام.

از دیرباز امنیت اطلاعات مورد توجه بوده و همواره تلاش بر این بوده است که از اطلاعات مهم و حساس به دقت محافظت نمایند. این تلاش غالباً در راستای عدم افشای اطلاعات بوده که می‌بایست محرمانه بماند و خصوصاً در زمان‌هایی مثل جنگ‌ها اهمیت حفظ آن‌ها به چندین برابر می‌رسیده است. شاید در گذشته به تمامیت و بقاء اطلاعات توجه چندانی نمی‌شد، لکن کم کم اهمیت و ارزش خود اطلاعات علی‌الخصوص در جوامع اطلاعاتی کنونی، جهت حفاظت و دور بودن از تخریب و امحاء، در جوامع بیشتر مورد توجه قرار گرفته است (تبریزی و همکاران، ۷:۱۴۰۲).

جوامع اطلاعاتی مبتنی براطلاعات سودمند بوده و بقاء اطلاعات نیزدر گرو حفظ امنیت و سلامت آن‌ها می‌باشد. به این جهت اهمیت اطلاعات فارغ از محتوایی که مورد انتقال قرار می‌دهند مشخص می‌گردد و داده‌های دیجیتالی که به کمک فناوری رایانه‌ای ایجاد و تکثیر می‌شوند در جوامع اطلاعاتی اهمیت بسیاری پیدا نموده‌اند. آنچه که به سیستم‌های رایانه‌ای و امنیت اطلاعات اهمیت فوق‌العاده بخشیده است همانا گسترش فضای اینترنت می‌باشد. به اشتراک گذاشتن اطلاعات در اینترنت و اهمیت بالای آن که استفاده از پایگاه‌های داده اینترنت و بانک‌های اطلاعاتی در حوزه‌های مختلف خدمات قضایی، اطلاع رسانی، ارتباطات، آموزش الکترونیک، تجارت الکترونیک و مصادیقی از این دست دارند، در نگرشی گسترده و کلان، اهمیت اطلاعات را مشخص می‌نماید. پژوهشگران در چند دهه اول ظهور شبکه اینترنت، از آن برای ارسال پست الکترونیک استفاده می‌نمودند. و کارمندان شرکت‌ها آن را برای (به اشتراک‌گذاری) چاپگرها مورد استفاده قرار می‌دادند. لذا امنیت در این سطح از استفاده مورد توجه چندانی واقع نمی‌شد، لکن امروزه که میلیون‌ها نفر از شهروندان و اشخاص از شبکه برای فروش، بانکداری، پرداخت مالیات‌ها و بهره‌گیری از خدمات قضایی استفاده می‌کنند امنیت داده‌ها یک مسئله جدی می‌باشد.

امروزه با تلاش و صرف هزینه‌های مالی و زمانی، نرم‌افزارهایی در زمینه رایانه، که نتیجه تلاش فکری دانشمندان زیادی می‌باشد تولید می‌شود و به بهانه زیادی از جمله توسعه حرفه‌ای و سرگرمی و غیره توسط کاربران که به آن‌ها نیاز دارند خریداری می‌شود. به همین شکل فایل‌های محتوایی همچون فایل‌های صوتی، نوشتاری و تصویری افراد امکان دارد حاصل زحمت و تلاش آنان در سالیان متمادی باشد. همینطور ارزش و اهمیت اطلاعات به میزان تعلق جوامع به اطلاعات بستگی دارد؛ در حقیقت هر میزان جامعه اطلاعاتی‌تر باشد به همان میزان در آن جامعه اطلاعات از اهمیت بیشتری برخوردار هستند. اهمیت اطلاعات در هر کشوری را می‌شود از کمیت و کیفیت قوانین مصوبه آن کشور در این حوزه درک نمود؛ نمونه‌ای از این قوانین در یک کشور، قوانین پیشرفته و مترقی کپی رایت می‌باشد؛ به طور مثال در کشورهای پیشرفته که مالکیت فکری اشخاص به شدت مورد حمایت واقع می‌شود، یک نسخه از نرم‌افزار سیستم عامل ویندوز، به بهای واقعی آن قابل خریداری است و قوانین نیز به شدت با نقض حقوق مؤلف از آن حمایت می‌کنند. اما در کشورهایی که برای حمایت از مالکیت معنوی ارزش چندانی قائل نبوده‌اند یا اصلاً مالکیت معنوی در این کشورها مورد حمایت قرار نمی‌گیرد همین نرم‌افزار به ثمن خیلی کم تر از ثمن واقعی آن و یا حتی به صورت رایگان قابل خریداری یا تهیه است؛ و در این زمینه در آن کشورها نه قانونی وجود دارد و یا اگر قانون نیم‌بندی هم وجود داشته باشد نیروهای قضایی و انتظامی اهمیت چندانی به این مسئله نمی‌دهند.(تبریزی و همکاران، ۱۴۰۲:۸)

افرادی که در بستر اینترنت و رایانه در پی انجام جرم و بالاخص خرابکاری و جرایم علیه امنیت هستند، عموماً از ابزارهای متعددی برای این کار استفاده می‌کنند. از جمله مهم‌ترین این ابزارها می‌توان به موارد ذیل اشاره کرد:

بدافزار: اصطلاح «نرم‌افزار بدافزار» می‌تواند به معنی هر تکه‌ای از کد رایانه باشد که تأثیری مغرضانه یا ناخواسته بر روی یک سیستم IT یا شبکه دارد. در حالی که بدون اغراق، هزاران مثال منحصر به فرد از نرم افزار بدافزار وجود دارد، دسته بندی کلیدی اساسا به صورت زیر در نظر گرفته می‌شود:

ویروس: یک برنامه تکثیر که توسط آلوده کردن اجسام «حامل» مانند دیسک‌ها، فایل‌ها یا اسناد وارد یک سیستم می‌شود. یک ویروس ممکن است بار مفیدی را حمل کند که در نقاطی بعد از آلودگی فعال خواهند شد و موجب اثرات ناخواسته و اغلب آسیب‌زا می‌گردد. این که لغت «ویروس» اغلب به غلط به عنوان یک برچسب عمومی برای همه اشکال نرم افزار بدافزار مورد استفاده قرار می‌گیرد بی‌ارزش است. این موضوع اغلب در متن گزارشات رسانه‌ای اتفاق می‌افتد و

این حقیقت که کاربرهای پایانی بسیاری همه اشکال نرم افزار بدافزار را مترادف با مفهوم یک ویروس درنظر می‌گیرند را بازتاب و توضیح می‌دهد.

ویروس رایانه‌ای در واقع کد مخرب رایانه‌ای می‌باشد که قادر به کپی‌سازی از خود و گسترش نمونه‌های متفاوت از خود را به داخل کدهای قابل اجرای دیگر، شبکه و برنامه‌های نرم افزاری یا اسناد رایانه‌ای، داراست. حافظه و فضای رایانه را با استفاده از برنامه‌های مجاز اشغال می‌نمایند، نتیجتاً آن‌ها به صورت عمومی موجب بروز رفتارهای نامتعارف از سامانه و اختلال در آن می‌شود. به طور کلی انواع آثار تخریبی ویروس‌ها و بدافزارهای رایانه‌ای عبارتند از: ایجاد اختلال درسامانه، شبیه سازی خطا، تخریب سخت افزار.

کرم: «کرم‌ها، گروه دیگر از کدهای مخرب، می‌باشند، که برخلاف ویروس‌ها قادر به تکثیر خود بدون شناسایی کد مستقر روی رایانه میزبان نمی‌باشند. معمولاً کرم‌ها از انتقال فایل‌ها بر روی خود رایانه یا شبکه استفاده کرده و نتیجتاً پهنای باند شبکه‌های رایانه‌ای را محدود و به آن‌ها آسیب می‌رساند».

کرم‌ها با اشتراک یک شباهت ظاهری با ویروس در مورد تکثیر میان سیستم‌های شبکه شده، از این نظر متفاوتند که آن‌ها قادر به انتشار به صورت مستقل، بدون نیاز به آلوده کردن یک حامل به روش یک ویروس هستند. کرم‌ها از اتصال شبکه‌ای میان سیستم‌ها سود می‌برند و می‌تواند به عنوان نتیجه‌ای از فعالیت کاملاً اتوماتیک شده (مثلاً اسکن آدرس‌های IP تصادفی و بهره برداری از آسیب‌پذیری‌ها جهت وارد شدن به سیستم‌های دور دست (یا اقدامات به اجرا درآمده توسط کاربر) مثلاً باز کردن مضامین جعلی از ضمیمه ایمیل یا اشتراک فایل‌های جفت جفت) انتشار یابد. آن‌ها در یک رایانه مقیم می‌شوند و فضای رایانه را اشغال نموده تا آنکه رایانه کند شود و یا کارایی خود را از دست بدهد.

بنابراین کرم یک عامل خود مختار است که از طریق خودش تکثیر می‌شود در حالی که ویروس خود را به نرم‌افزارها می‌چسباند و با اجرای آن نرم افزار تکثیر می‌شود (ضیایی پرور، ۱۹۷:۱۳۸۳). غالباً کرم‌ها را به دو دسته تقسیم می‌کنند: کرم‌های میزبان و کرم‌های شبکه‌ای.

کرم‌های رایانه‌ای در کشورهایی که از فناوری رایانه و سیستم‌های امنیتی پیشرفتگی کمتری دارند، تهدیدی به مراتب شدیدتر تلقی می‌شود.

اسب تروجان: این دسته از بدافزارها که نام خود را از اسب چوبی میان‌تهی مورد استفاده یونانیان جهت هجوم به تروا گرفته است. به برنامه‌هایی اشاره دارد که کاربر را برای به اجرا در آوردن خود توسط تظاهر به انجام یک دستورالعمل مشخص فریب می‌دهد اما در نهایت مشخص می‌شود که

در حال انجام کاری دیگر (در عوض دستورالعمل مورد ادعا یا علاوه بر آن) می‌باشد که منجر به تأثیرات غیر منتظره و اساسا ناخواسته می‌شود.

نرم‌افزارهای جاسوسی: این‌ها نرم‌افزارها نه کرم‌اند و نه ویروس ، بلکه نرم‌افزارهایی می‌باشند که در بسیاری از مواقع توسط شرکت‌های تبلیغاتی مورد سوء استفاده قرار می‌گیرند؛ «ادورها» و «اسپایورها» جاسوسانی هستند که نه تنها تبلیغات بنر را بر روی صفحات رایانه نشان می‌دهند بلکه عادات وب گردی کاربران را نیز پیگیری می‌کنند و بعد از آن به شرکت‌های تبلیغاتی اطلاع می‌دهند. این شرکت‌ها هم وقتی می‌بینند که به عنوان مثال شما بیشترین مراجعه‌تان به سایت‌های گردشگری بوده است، تبلیغاتی را با مضمون‌های مشابه به صورت نواری در بالا یا پایین صفحه کامپوتر هنگامی که کاربر در حال گشتزنی در اینترنت است، به نمایش می‌گذارند. این برنامه‌ها به طور رایگان قابل دسترس‌اند و می‌توان آن‌ها را بر روی سیستم عامل خود نصب نمود؛ هر چند گاهی اوقات این نرم‌افزارها با نیات و مقاصد منفی توسط شرکت‌های تبلیغاتی استفاده نمی‌شوند، اما در اکثر مواقع کاری جز جاسوسی و خرابکاری ندارند. یکی از مشکلات رایجی که آن‌ها به وجود می‌آورند کاهش سرعت سیستم عامل نصب شده می‌باشد و درپاره‌ای اوقات آنقدر حجم فعالیتشان زیاد می‌شود که می‌توانند سیستم عامل را مختل و غیرقابل کاربری نمایند.(نادرخانی، ۱۳۹۰:۵۰)

همه موارد مذکور می‌تواند تهدیدی برای شبکه خدمات رسانی قضایی الکترونیک باشد و علیرغم تأثیرگذاری این شبکه بر کاهش اطاله دادرسی امنیت و روند رسیدگی‌ها را با مشکل مواجه کند لذا از جمله اقدامات برای پیشگیری از وقوع چنین مواردی بهره‌گیری از پیشگیری وضعی اعم از کاهش فرصت‌های ارتکاب است.

نتیجه گیری

ضرورت بهره‌گیری از ابزارهای الکترونیکی در انواع دادرسی‌ها و ارائه خدمات الکترونیک قضایی کمک بزرگی برای پیشگیری از اتلاف انرژی، هزینه‌های غیر ضروری، وقت و نیز فوریت احقاق حق در جهت رسیدن به دادرسی عادلانه بوده است. قانونگذار کشور ایران نیز به موازات گسترش فناوری اطلاعات و ارتباطات مبادرت به تصویب قانون آیین دادرسی الکترونیکی نموده است که خود گامی مهم و اساسی در گسترش دادگستری الکترونیک می‌باشد لکن اجرای این قانون در حال حاضر با چالش‌های متعددی مواجه است و علیرغم تأثیرات مثبتی که دادرسی الکترونیک داشته است، اجرای آن در نظام حقوقی ایران به شکل کارآمد و صحیح آن با نواقص و کاستی‌هایی همراه است و اجرای آن مطابق با امکانات زیرساختی موجود در برخی موارد به نحو شایسته صورت

نمی‌گیرد. به صورت عمده، این نواقص و کاستی‌ها مربوط به به ضعف زیرساخت‌های ضروری و مورد نیاز، مثل نبود زیرساخت‌ها و امکانات تکنولوژیکی به روز و کامل و سرعت کند اینترنت و احتمال سوء استفاده اشخاص ثالث از عدم آگاهی افراد و آشنا نبودن اشخاص با این نوع از روند رسیدگی، می‌باشد.

یکی از مهم‌ترین چالش‌های پیش روی ارائه خدمات الکترونیک قضایی موضوع امنیت داده‌ها می‌باشد که با توجه به این واقعیت که دادگاه‌ها با حجم وسیعی از داده‌های حساس تجاری و حتی اسرار دولتی سروکاردارند، موضوع امنیت در زمینه دادگاه‌های آنلاین از اهمیت ویژه ای برخوردار است. همچنین یکپارچگی داده‌های پردازش و ذخیره شده نیز باید مدنظر قرار گیرد و حوزه‌های قضایی که توسعه دادگاه‌های آنلاین را در نظر می گیرند باید به دنبال شناسایی بهترین راه‌حل‌های فنی باشند. به عنوان مثال احراز هویت لایه‌ای کاربر وآموزش مداوم در مورد مسائل امنیتی از جمله روش هایی است که می تواند برای به حداقل رساندن ریسک‌های امنیتی در نظر گرفته شود. سیستم‌های نظارت بر پایگاه داده برای اطمینان از یکپارچگی داده‌ها از طریق تست‌های امنیتی باید در اولویت باشد. اگر چه سیستم‌های دیجیتال در بسیاری از موارد از سیستم‌های کاغذی قدیمی ایمن‌تر هستند چرا که از دست دادن، سرقت و یا تخریب داده‌ها در سیستم‌های سنتی می تواند امری عادی باشد. ثانیاً، باید در سیاستی که به دنبال مدیریت ریسک است، به جای دوری از بکارگیری فناوری، تعادلی ایجاد کرد.

همچنین یکی از فناوری‌های نوین که می‌تواند کمک کننده به دادرسی الکترونیک باشند تا طیفی از چالش‌های پیش رو را برطرف نماید، فناوری زنجیره‌های بلوکی می‌باشد.

با توجه به طیف وسیع کاربردهایی که فناوری زنجیره بلوکی دارد، قابلیت تغییر زندگی روزمره بشر به صورت بنیادین را دارد. عمده‌ای از قوانین و مقررات جاری کشور که تصور می‌شد خنثی نسبت به فناوری هستند، قابل تجدیدنظر پس از عملیاتی شدن کامل و جامع فناوری زنجیره بلوکی خواهند بود. اعتماد ناگزیر به بشر و نهادهای قدیمی بشری، جای خود را به اعتماد روزافزون به فناوری‌های رایانشی خواهد داد و نظام‌های ملی از حالت متمرکز به سمت توزیع شدگی حرکت می‌کنند. به نحوی که نهادهای مدنی متمرکز همچون مراجع قضایی کم کم جای خود را به نهادهای توزیع شده کم هزینه‌تر و چابک‌تر رایانه‌ای می‌دهند.

در موارد بسیاری از خدمات الکترونیکی همچون خدمات الکترونیک قضایی هم اکنون به دلایل مختلف حقوقی و غیر حقوقی همانند عدم اعتماد دستگاه‌ها به یکدیگر از پیشرفت‌های کافی بهره‌مند نگشته‌اند و یا حتی کنار گذاشته شده و از بهره‌مندی از آن صرف نظر نموده‌اند. فناوری

زنجیره بلوکی این قابلیت را دارد که اعتماد و تفاهم را میان دستگاه‌ها جاری سازد و جریان اطلاعات لازم میان دستگاه‌ها برای تحقق دولت الکترونیکی و الکترونیکی شدن خدمات در ارتقای زمینه‌هایی همانند حوزه قضایی و در حوزه‌هایی که تا کنون قابل الکترونیکی کردن نبوده را نیز فراهم نماید.

در واقع دولت و قوه قضاییه از فناوری زنجیره‌های بلوکی برای پوشاندن شکاف‌های تکنولوژیک بهره می‌برند و با استفاده از فناوری‌های نوین که برای رشد و پایداری بسیار مهم بوده جهت حفاظت از داده‌ها و اطلاعات قضایی بهره می‌گیرند.

بنابراین پیشنهاد می‌شود نوعی سیستم ثبت اطلاعات در دستگاه‌های قضایی ایجاد گردد که بر پایه فناوری بلاک چین کار کند. این سیستم قرار است میان تمام اعضای شبکه که به آن متصل هستند به اشتراک گذاشته شود و اطلاعات آن از طریق یک بلاک به بلاک دیگر منتقل شود. این اطلاعات تنها به صورت رمزنگاری شده قابل انتقال هستند.

دادگاه‌ها نیز می‌توانند از بلاک چین برای کمک به رسیدگی به حداقل سه چالش مهم در نگهداری سوابق دادگاه، مدیریت احکام دادگاه، حکم‌ها و سوابق جنایی استفاده کنند.

منابع و مآخذ

استیون هیک، ادوارد، هلپین، اف، هوسکنیز، اریک (۱۳۸۶). حقوق بشر و اینترنت. ترجمه و تحقیق دکتر سید قاسم زمانی و مهناز بهراملو، تهران: انتشارات خرسندی.

السان، مصطفی (۱۳۹۳). حقوق تجارت الکترونیکی. چاپ دوم، تهران: سمت.

بامبارا، جوزف جی، آلن، پل آر (۱۳۹۹). کاربردهای بلاک چین برای توسعه کسب و کارها، قانون، فناوری و بانکداری، بابل: علوم رایانه.

به‌گذر، حمیدرضا (۱۴۰۲). دادرسی الکترونیک و جایگاه آن در نظام حقوقی ایران، مجله حقوقی و قضایی.

تبریزی، صادق، الهی منش، محمدرضا، عالی پور، حسن، طهماسبی، جواد (۱۴۰۲). توقیف داده‌ها و سامانه در جرایم امنیتی؛ چالش‌ها و معیارها، فصلنامه علمی امنیت ملی.

رجبی، ابوالقاسم، فریور، روح‌الله (۱۱۳۹۶). آشنایی با فناوری راهبردی زنجیره بلوکی و کاربردهای آن». مطالعات ارتباطات و فناوری‌های نوین (گروه ارتباطات و فناوری اطلاعات) به درخواست معاونت پژوهش‌های زیربنایی و امور تولیدی.

رضایی‌نژاد، همایون، محسنی، حسن (۱۳۹۱). دادگستری و پیشرفت فن‌آوری اطلاعات و ارتباطات، نشریه مطالعات حقوقی، دوره چهارم، شماره ۲.
شهبازی نیا، پرویز، غمامی، مجید، جوان، صدیقه (۱۳۹۶). فناوری اطلاعات و ارتباطات و عدالت قضایی. فصلنامه دیدگاه‌های حقوق قضایی، شماره ۸۰-۷۹.
صادقی، حسین (۱۳۸۶). حمایت از حریم خصوصی اطلاعاتی و ارتباطاتی در اسناد بین‌المللی و حقوق ایران. اولین کنفرانس بین‌المللی شهر الکترونیک.
کهن هوش نژاد، روح الله، پاک زاد، سید مهدی (۱۳۹۷). اقتصاد بلاک چین، تهران: چالش.
مؤذن زادگان، حسنعلی، روستا، نرجس (۱۳۹۶). دادرسی الکترونیکی در رویارویی با جرائم رایانه‌ای: چالش‌ها و بایسته‌ها. مجله حقوقی دادگستری، شماره ۱۰۰.
مهرافشان، علیرضا (۱۳۹۰). دادرسی مجازی مفهومی نوین در عدالت قضایی. مطالعات فقه و حقوق اسلامی، سال سوم، شماره ۵.
نادرخانی، نیما (۱۳۹۰). ابزارهای مورد استفاده مجرمان و خرابکاران رایانه‌ای. نشریه کارآگاه، شماره ۱۴.
یوسفی، عبدالعزیز، جلیل مژدهی، مژده، پاینده، محمد (۱۴۰۰). کاربرد بلاک چین در کسب و کارها، تهران: ادبستان.