مقاله

مجله

پژوهشهای حقوقی

شماره ۱۶

هزار و سیصد و هشتاد و هشت ـ نیمسال دوم

مقالات

- دسترسی به وکیل در مرحله تحقیقات پلیسی
- حق بایع برای رفع عیب مبیع در کنوانسیون بیع بین‌المللی کالا و حقوق ایران
- مسؤولیت مدنی در قبال حوادث طبیعی (بررسی تطبیقی مبانی، محدودیت‌ها و رویه قضایی با تأکید بر زلزله)
- فسخ قرارداد کار در حقوق ایران پیش و پس از تصویب قانون رفع برخی از موانع تولید و سرمایه‌گذاری
- اجرای فراسرزمینی میثاق بین‌المللی حقوق مدنی و سیاسی با تکیه بر رویه کمیته حقوق بشر
- سیستم اطلاعاتی مطمئن در قانون تجارت الکترونیکی
- رویکرد متعارض دولت‌ها به حق تعیین سرنوشت خارجی: بررسی نظریات دولت‌ها در قضیه کوزوو
- ملاحظاتی بر شورای قانون اساسی فرانسه
- «رفتار عادلانه و منصفانه» دولت میزبان با پیمانکاران خارجی
- غرامت در دعاوی ناشی از قرارداد سرمایه‌گذاری خارجی (غیر از سلب مالکیت)
- کمیسیون حقوق بین‌الملل سازمان ملل متحد و منابع طبیعی مشترک

موضوع ویژه: حقوق نفت و گاز در نظام ملی و بین‌المللی

- چرا حقوق نفت و گاز؟
- پیوند میان بخش انرژی و مقررات سازمان جهانی تجارت
- ثبات قراردادی با تأکید بر نمونه قراردادهای اکتشاف و استخراج نفت
- شرکت‌های نفتی و معضل اعمال حمایت دیپلماتیک توسط ایران
- مالکیت خصوصی بر منابع نفت و گاز در حقوق ایالات متحد امریکا
- حل اختلافات سرمایه‌گذاری در معاهده منشور انرژی و آثار حقوقی الحاق ایران به آن

نقد و معرفی

- تأملی انتقادی بر لایحه «آیین دادرسی دیوان عدالت اداری»
- نقد و ارزیابی طرح نمایندگان مجلس جهت انتقال و دوره‌ای کردن مقر سازمان ملل متحد
- اجلاس کپنهاگ (۲۰۰۹) و ضرورت مقابله با تغییرات آب و هوایی

شهر دانش

مؤسسه مطالعات و پژوهشهای حقوقی

شاپا: ۱۶۸۲-۹۲۲۰

http://jlr.sdil.ac.ir/article_41642.html

مجله پژوهشهای حقوقی (علمی ـ ترویجی)، شماره ۱۶، نیمسال دوم ۱۳۸۸
صفحات ۱۲۳ الی ۱۳۱، تاریخ وصول: ۱۳۸۸/۱/۳۱، تاریخ پذیرش: ۱۳۸۸/٤/۱٤

سیستم اطلاعاتی مطمئن در قانون تجارت الکترونیکی

محبوبه عبدالهی*
دکتر مرتضی شهبازی‌نیا**

چکیده: به موجب قانون تجارت الکترونیکی، یکی از ضروریات تحقق دلیل الکترونیکی مطمئن، سیستم اطلاعاتی مطمئن است.سیستم اطلاعاتی مطمئن، سیستمی است که در ایجاد، ذخیره و انتقال داده‌پیام به صورتی عمل نماید که به هنگام لزوم در دسترس باشند و از طرفی به گونه‌ای سازماندهی شود که با جلوگیری از هرگونه نفوذ و سوء استفاده، تمامت و محرمانگی اطلاعات را تضمین کند. ابزارهای الکترونیکی پویا بوده و دائماً در حال تغییرند به همین جهت قانون تجارت الکترونیکی، یک فناوری خاص را به عنوان سیستم اطلاعاتی مطمئن معرفی نکرده است بلکه کارکردهای چنین سیستمی را ارائه کرده است و هر سیستمی که دارای کارکردهای مذکور باشد سیستم مطمئن محسوب می‌شود. در این مقاله، شرایط سیستم اطلاعاتی مطمئن در قانون تجارت الکترونیکی را بررسی کرده، با نحوه احراز این شرایط آشنا می‌شویم.

کلیدواژه‌ها: سیستم اطلاعاتی، امنیت اطلاعات، تجارت الکترونیکی، قانون تجارت الکترونیکی، دلیل الکترونیکی

* کارشناس ارشد حقوق خصوصی دانشگاه تربیت مدرس Email: m_abdolahi_80@yahoo.com
** استادیار دانشگاه تربیت مدرس Email: shahbazinia@modares.ac.ir

۱. مقدمه

سیستم اطلاعاتی، سیستمی برای تولید، ارسال، دریافت، ذخیره یا پردازش داده‌پیام است. صحت و اطمینان دلیل الکترونیکی به سطح ایمنی سیستم اطلاعاتی که در فرایند ایجاد، ذخیره و انتقال آن نقش داشته است، بستگی دارد، در صورتی که این سیستم در مقابل رخنه و نفوذ، ایمن و از دقت و اطمینان کافی برخوردار باشد، می‌توان از صحت اطلاعاتی که توسط این سیستم به وجود آمده‌اند، اطمینان حاصل کرد.

قانون تجارت الکترونیکی، دلایلی را که توسط سیستم‌های اطلاعاتی مطمئن ایجاد و ذخیره شده و دارای امضای الکترونیکی مطمئن هستند، دلیل مطمئن تلقی کرده و چنین ادله‌ای را غیرقابل انکار و تردید می‌داند.[۱]

با توجه به اینکه وجود چنین سیستمی از ضروریات تحقق دلیل مطمئن است، آشنایی با شرایط تحقق این سیستم، ضروری است که در این مقاله به بررسی این موضوع می‌پردازیم.

۲. تعریف سیستم اطلاعاتی مطمئن

سیستم اطلاعاتی، سیستمی برای تولید (اصل‌سازی)، ارسال، دریافت، ذخیره یا پردازش «داده‌پیام» است و شامل تمام انواع سخت‌افزار، نرم‌افزار و یا شبکه‌های ارتباطی است؛ بنابراین یک صندوق پستی الکترونیکی[۲] یا حتی دستگاه نمابر می‌تواند یک سیستم اطلاعاتی باشد.

سیستم اطلاعاتی مطمئن، سیستمی است که اطلاعات را به گونه‌ای ذخیره کند که به هنگام لزوم در دسترس باشند و از طرفی به گونه‌ای سازماندهی شود که با جلوگیری از هرگونه نفوذ و سوء استفاده، تمامت و محرمانگی اطلاعات را تضمین کند[۳].

۳. شرایط تحقق سیستم اطلاعاتی مطمئن

با توجه به آنکه رخنه‌گرها همواره روش‌های جدیدی برای نفوذ به سیستم‌های اطلاعاتی

---

۱. محبوبه عبدالهی، «دلیل الکترونیکی در دعوای حقوقی»، **پایان‌نامه کارشناسی ارشد حقوق خصوصی**، دانشگاه تربیت مدرس، ۱۳۸۷، ص ٥٦.

2. Electronic Mail Box.

3. UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, aa: www.Uncitral.org/pdf/English/texts/electoms/ml-e common.html.N.40.

ایجاد می‌نمایند، ابزارهای الکترونیکی و شیوه‌های حفاظت از سیستم نیز پویا بوده و متناسب با این نیاز تغییر می‌کنند، به همین جهت معرفی یک زیرساخت فنی ثابت به عنوان یک سیستم مطمئن امکان ندارد بلکه برای حفظ امنیت سیستم باید روش‌های حفاظت از سیستم، به روزرسانی شود. با عنایت به این امر، قانون تجارت الکترونیکی معیارهای یک سیستم اطلاعاتی مطمئن را معرفی کرده است که تحقق آنها در هر زمان با توجه به تناسب اوضاع و احوال سنجیده می‌شود، بنابراین قانون تجارت الکترونیکی، نوعی بیطرفی در فناوری را اتخاذ کرده است که این امر موجب پویایی قانون می‌شود.[4]

شرایط تحقق سیستم اطلاعاتی مطمئن در بند ح ماده ۲ قانون تجارت الکترونیکی تعیین شده است. این بند مقرر می‌دارد:

«سیستم اطلاعاتی مطمئن سیستم اطلاعاتی است که:

به نحوی معقول در برابر سوء استفاده و نفوذ محفوظ باشد.

سطح معقولی از قابلیت دسترسی و تصدی صحیح را دارا باشد.

به نحوی معقول متناسب با اهمیت کاری که انجام می‌دهد پیکربندی و سازماندهی شده باشد.

موافق با رویه ایمن باشد.»

قانون‌گذار محفوظ بودن در برابر سوء استفاده و نفوذ، قابلیت دسترسی و تصدی صحیح، پیکربندی و سازماندهی و رویه ایمن را شروط سیستم اطلاعاتی مطمئن می‌داند که در زیر به بررسی آنها می‌پردازیم.

۱-۳. محفوظ بودن در برابر نفوذ و سوء استفاده

منظور از «سوء استفاده»، استفاده غیرمجاز از سیستم است که ممکن است توسط افراد داخل شبکه یا اشخاص ثالث صورت گیرد.

«نفوذیابندگی» به معنای دسترسی افراد رخنه‌گر از طریق شبکه یا محیط فیزیکی سیستم‌های اطلاعاتی است. در صورتی که سیستم در مقابل این خطرات محافظت نشود ممکن است اطلاعات فاش شده، یا تغییر پیداکرده و حذف شوند به همین جهت باید سیستم در مقابل این خطرات کنترل شود.[5]

4. United National, Convention On The Use Of Electronic Communications In International Contract 2007, www.uncitral.org. N. 151.

5. Federal Financial Institution Examination Council, information security, aa: http://www.ffiec.gov/ffiecinfobase/booklets/information_security/informatp.72.

کنترل سیستم غالباً از سه طریق اداری، تکنیکی و فیزیکی انجام می‌شود.[۶]

برای کنترل اداری، سیستم باید به گونه‌ای طراحی شود که تنها اشخاص واجد صلاحیت برحسب وظیفه‌شان و در همان حد اجازه ورود به سیستم را داشته باشند؛ تصدیق هویت افراد مجاز از طرقی همچون استفاده از کارت هوشمند، گذر واژه، شماره شناسایی شخصی و یا ویژگی‌های زیست سنجی همچون سنجش اثر انگشت، تصویر عنبیه چشم، صدا یا کف دست انجام می‌شود.[۷]

به منظور کنترل تکنیکی سیستم از نرم‌افزارهایی همچون دیواره آتش[۸]، سیستم‌های کشف ورود غیرمجاز به سیستم[۹] و رمزنگاری داده‌ها[۱۰] جهت حفاظت سیستم استفاده می‌شود.

نفوذ به شبکه گاه از طریق محیط فیزیکی سیستم‌ها صورت می‌گیرد بنابراین محیط کار باید از دسترسی اشخاص ثالث مصون باشد. برای ایمنی محیط باید از قفل‌ها، درها، دوربین‌ها و سیستم‌های کنترل عبور استفاده کرد؛ به منظور حفظ امنیت و سلامت دستگاه‌ها، محیط کار باید مجهز به ابزارهای خنک‌کننده و گرم‌کننده، هشداردهنده‌ها و سیستم‌های مهار آتش‌سوزی باشد. همچنین نمایش اطلاعات روی صفحه نمایشگر در حضور اشخاص ثالث می‌تواند منجر به فاش شدن اطلاعات شود که با نرم‌افزارهای ویژه-ای می‌توان از نمایش اطلاعات جلوگیری کرد.[۱۱]

---

6. *Ibid*, p. 63.

7. University of California Business and Finance Bulletin,"IS-3 Electronic Information Security", 2008, p. 12. aa: http://people.seas.harvard.edu/~tmoore/science-econ.pdf

۸. Fire Wall نوعی سیستم امنیتی است که شبکه را در مقابل مهاجمان خارج از شبکه سازمانی که غالباً از طریق اینترنت وارد شبکه می‌شوند حفاظت می‌کند. دیوار آتش ارتباط مستقیم رایانه‌های شبکه را با شبکه‌های بیرونی همچون اینترنت قطع می‌کند. و کلیه ارتباطات داخل شبکه به خارج از آن و بالعکس باید از یک محیط واسط عبور نماید، و این محیط کلیه ارتباطات را کنترل می‌کند. محسن شجاعی و احمد ملکی‌زاده، **تجارت الکترونیکی**، انتشارات پرتونگار، ۱۳۸۳، ص ۱۲۵.

۹. Network Instruction Detection System این سیستم می‌تواند ورود رخنه‌گر به سیستم را تشخیص دهد برخی دیگر از این سیستم‌ها موسوم به «تأییدکننده‌های صحت سیستم» زمان تغییر پوشه توسط رخنه‌گر را نیز تشخیص می‌دهند. سهیل سرمدسعیدی و وحیدرضا میرابی، **تجارت الکترونیکی**، کیمیا، ۱۳۸۳، ص ۲۴۸.

۱۰. Encryption منظور از رمزنگاری داده‌ها ارسال اطلاعات به گونه‌ای است که بدون داشتن کلید رمزگشای مربوطه امکان خواندن پیام یا بازگشایی پیام وجود ندارد.

Henry Wolfe, "Forensics and the Emerging Importance Evidence Gathering", p. 12, aa: http://nzcs.org.nz/sITE-Default/x-files/4915 pdf, 2001.

11. University of California, *op. cit.*, p. 19.

۲-۳. قابلیت دسترسی[۱۲] و تصدی صحیح[۱۳]

«قابلیت دسترسی» سیستم اطلاعاتی به آن معناست که سیستم خارج از سرویس نباشد و کارآیی سیستم و کنترل‌های امنیتی آنها به گونه‌ای باشد که هنگام نیاز به اطلاعات بتوان از آنها استفاده کرد[۱٤].

«تصدی صحیح» به معنای آن است که مدیریت و سازماندهی نیروی انسانی به شیوه‌ای باشد که امنیت سیستم حفظ شود و وظایف اشخاص باید به گونه‌ای تفکیک شود که امکان سوء استفاده آنان از اختیاراتشان کمتر شود برای مثال کسی که وظیفه درخواست پرداخت چک را به عهده دارد نباید شخصاً قادر به پرداخت آن باشد یا کسی که برنامه‌های کاربردی مانند برنامه حسابداری یک شرکت را طراحی می‌کند نباید خود مدیر سرور یا مدیر پایگاه داده باشد. می‌توان سیستم را به گونه‌ای طراحی کرد که هر شخص فقط در حیطه وظایفش قدرت دسترسی به سیستم را داشته باشد.[۱۵]

۳-۳. پیکربندی[۱٦] و سازماندهی[۱۷]

پیکربندی سیستم به معنای جمع سخت‌افزار داخلی و خارجی آن شامل حافظه، دیسک-گردان، صفحه کلید، سخت افزارهای اضافی مانند ماوس، مودم و چاپگر و نیز چگونگی ارتباط یافتن عناصر یک شبکه اطلاعاتی با یکدیگر است[۱۸]. نوع سخت‌افزار مورد استفاده و سازماندهی آن باید کارآیی کافی برای انجام کار مورد نظر را داشته باشد مثلاً اگر انتظار می‌رود که سیستم با سرعت بالا عمل کند باید از سخت‌افزاری استفاده شود که این نیاز را برآورده کند یا اگر سیستم برای انجام محاسبات پیچیده و حجیم استفاده می‌شود سخت‌افزار باید ازحافظه قوی‌تری برخوردار باشد.

٤-۳. موافق بودن با رویه ایمن

بند «ط» ماده ۲ قانون تجارت الکترونیکی رویه ایمن را چنین تعریف کرده است: «رویه‌ای است برای تطبیق صحت ثبت «داده پیام» و منشأ و مقصد آن با تعیین تاریخ و برای یافتن

12. Availability
13. Management
14. University of California Business and Finance Bulletin, *op. cit.*, p. 5.
15. Federal Financial Institution Examination Council, *op. cit.*, p. 63.
16. Configuration
17. Organization

۱۸. فرهنگ تشریحی میکروسافت، ذیل واژه مذکور.

هرگونه خطا یا تغییر در مبادله، محتوا و یا ذخیره‌سازی داده‌پیام از یک زمان خاص. یک رویه ایمن ممکن است با استفاده از الگوریتم‌ها، کدها، کلمات یا ارقام شناسایی، - رمزنگاری، روش‌های تصدیق یا پاسخ برگشت و یا طرق ایمنی مشابه انجام شود».

شرط ایمن بودن با استفاده از یک امضای دیجیتال به‌خوبی تأمین می‌شود. امضای دیجیتالی که توسط مراجع گواهی صادر شده باشد منشأ و مقصد داده‌پیام را به شیوه‌ای غیرقابل انکار تعیین می‌کند همچنین این امضا با استفاده از عمل «خرد کردن»[19] و ایجاد خلاصه داده‌پیام به گونه‌ای عمل می‌کند که هرتغییر ایجادشده در پیام قابل‌کشف است. این امضا مجهز به «مهر زمان»[20] می‌باشد که تاریخ صدور امضا را تعیین می‌نماید.

قانون‌گذار وجود «سطح معقولی» از شرایط مذکور را برای اطمینان یک سیستم اطلاعاتی لازم می‌داند. با توجه به معیار «سنجش معقول»[21] که در بند «ن» ماده ۲ قانون تجارت الکترونیکی ارائه شده است، شرایط مذکور با توجه به اوضاع و احوال مبادله داده‌پیام از جمله طبیعت مبادله، مهارت و موقعیت طرفین، حجم مبادلات طرفین در موارد مشابه، در دسترس بودن گزینه‌های پیشنهادی و رد آن گزینه‌ها از جانب هریک از طرفین، هزینه گزینه‌های پیشنهادی، عرف و روش‌های معمول و مورد استفاده در این نوع مبادلات ارزیابی می‌شود.

بنابراین در یک معامله کم بها، سیستمی که از سطح ایمنی پایینی برخوردار است، می‌تواند مطمئن محسوب شود زیرا استفاده از یک سیستم اطلاعاتی با سطح ایمنی بالا که مستلزم هزینه‌های سنگین است در چنین معاملاتی معقول نمی‌باشد. همچنین در یک شرکت کوچک که فقط یک نفر مأمور ثبت اسناد است، یک گذر واژه ساده، سطح معقولی از تصدی صحیح را تحقق می‌بخشد اما در یک شرکت بزرگ که دارای شبکه رایانه‌ای و سرور مرکزی است، تصدی صحیح در صورتی تحقق می‌یابد که حسابداران صرفاً در حیطه کاری خود به شبکه دسترسی داشته باشند و پس از ثبت اطلاعات توان تغییر آنها را نداشته باشند[22].

در صورتی که شخصی مدعی مطمئن بودن سیستم اطلاعاتی باشد در این مورد مدعی محسوب می‌شود زیرا اظهار او خلاف اصل است و به موجب قاعده «البینه علی المدعی» بار اثبات به عهده مدعی آن است و برای اثبات این امر باید وجود یک‌یک شرایط مذکور

19. Hash function
20. Time-Stamp
21. Reasonableness Test
22. UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, N. 86.

در بند ح ماده ۲ قانون تجارت الکترونیکی احراز شود، دادگاه برای احراز این موارد موضوع را به کارشناس ارجاع می‌دهد، احراز یک‌یک این موارد مستلزم صرف هزینه و زمان زیادی است که ممکن است شخصی که به سیستم اطلاعاتی مطمئن استناد می‌نماید به دلیل ناتوانی از اثبات، از پیروزی در دعوا محروم شود. برای معاف نمودن مدعی از این تکلیف دشوار، شایسته است برخی روش‌های فنی موجود که از شرایط اطمینان برخوردارند به عنوان امارات اطمینان دلیل معرفی شوند.

پیش‌نویس قانون تجارت الکترونیکی در ماده ۱۲۷ کمیته‌ای با عنوان کمیته فناوری و استاندارد سیستم‌های اطلاعاتی پیش‌بینی کرده بود تا با تحقیق در خصوص آخرین دستاوردهای علمی، بهترین روش‌های موجود را با انتشار راهنمای عمل معرفی نماید که روش‌های فنی معرفی شده بدون نیاز به اثبات اطمینان می‌توانستند در دادگاه مورد قبول قرار گیرد که متأسفانه این بند در تنظیم نهایی قانون حذف شد اما می‌توان با استفاده از نسخه‌های استاندارد و رویه‌های متحدالشکل از بار اثبات دعوا کاست.

سازمان بین‌المللی استانداردسازی (ISO)[۲۳]، متشکل از مؤسسه‌های استاندارد ملی از ۱۵۷ کشور دنیاست که قالب‌های مطمئن و پویا برای امنیت اطلاعات ارائه می‌کند. مهم‌ترین استانداردهایی که تاکنون توسط این مؤسسه ارائه شده‌اند عبارتند از:

ISO-15443: چارچوبی برای تضمین امنیت سیستم‌های اطلاعاتی ارائه می‌کند.

ISO-17799: دستورالعمل مدیریت یک سیستم اطلاعاتی مطمئن را معرفی می‌کند.

ISO-27001: برای تأمین امنیت سیستم‌های اطلاعاتی حرفه‌ای مفید است.

اجرای این استانداردها امکان سوء استفاده از اطلاعات و نفوذ به سیستم را به حداقل رسانده، قابلیت دسترسی سیستم، صحت داده‌ها و غیرقابل انکار بودن ارسال و دریافت اطلاعات را تضمین می‌نماید[۲۴].

یکی دیگر از استانداردهای معتبر دنیا، کتاب نارنجی استاندارد امریکاست که توسط وزارت دفاع امریکا اعلام شده است. نرم‌افزار و سخت‌افزار سیستم بر اساس این استاندارد به‌طور جداگانه بازرسی می‌شوند و دستگاه‌هایی که منطبق بر این استاندارد باشند تأییدیه دریافت می‌کنند.

کشورهای انگلستان و آلمان نیز دستورالعمل‌هایی را جهت استانداردسازی سیستم ارائه

23. International Organization for Standardization
24. Sudhanshu Kairab, *A Practical Guide to Security Assessments*, London, CRC Press Company, 2004, p. 229.

کرده‌اند و تولیدکنندگان نرم‌افزار و سخت‌افزاری که این دستورالعمل‌ها را مد نظر داشته باشند گواهی امنیت دریافت می‌کنند.

در کشورهای پیشرفته سیستم‌های رایانه‌ای که برای مبادلات اقتصادی و تجاری مورد استفاده قرار می‌گیرند داده‌ها را به صورت دسته‌ای ارسال می‌کنند، قبل از ارسال آنها کدهای کنترلی فعال و همراه داده‌ها ارسال می‌شوند، واحد پردازش مرکزی قبل از ارسال، آنها را امتحان می‌کند اگر نتایج امتحان صحیح نباشد ٢٤ امتحان دیگر صورت می‌گیرد تا نقص سیستم آشکار شود.[۲۵]

٤. نتیجه

برای اطمینان از صحت و تمامت دلیل، لازم است سیستمی که اطلاعات توسط آن تولید، ارسال، دریافت، ذخیره یا پردازش می‌شوند از اطمینان و ایمنی کافی برخوردار باشد. در حقیقت قانون تجارت الکترونیکی، در صورتی دلیل الکترونیکی را مطمئن تلقی می‌کند که توسط یک سیستم اطلاعاتی مطمئن ایجاد شده باشد. به موجب بند ح ماده ۲ قانون تجارت الکترونیکی، چنین سیستمی باید به نحوی معقول در برابر سوء استفاده و نفوذ محفوظ باشد، سطح معقولی از قابلیت دسترسی و تصدی صحیح را دارا باشد، متناسب با اهمیت کاری که انجام می‌دهد پیکربندی و سازماندهی شده باشد و موافق با رویه ایمن باشد تا به واسطه آن، اطلاعات همواره در دسترس باشند و تمامت و و محرمانگی آنها تضمین شود.

اثبات تمام شرایط مذکور به عهده شخصی است که مدعی مطمئن بودن سیستم اطلاعاتی است. این امر بار اثبات سنگینی را به عهده اثبات‌کننده گذاشته است اما می‌توان با استفاده از نسخه‌های استاندارد معرفی شده توسط مؤسسات معتبر از جمله سازمان بین‌المللی استانداردسازی از این بار اثبات کاست.

فهرست منابع

۱. سهیل سرمدسعیدی و وحیدرضا میرابی، تجارت الکترونیکی، کیمیا،۱۳۸۳.

۲. سیامک قاجار، ادله اثبات در محیط‌های دیجیتال، دبیرخانه شورای عالی انفورماتیک، چاپ محدود، ۱۳۷٤.

۲۵. سیامک قاجار، **ادله اثبات در محیط‌های دیجیتال**، دبیرخانه شورای عالی انفورماتیک، چاپ محدود، ۱۳۷٤، ص ۳٦.

۳. محسن شجاعی و احمد ملکی زاده، تجارت الکترونیکی، انتشارات پرتونگار،۱۳۸۳.
٤. محبوبه عبدالهی، دلیل الکترونیکی در دعوای حقوقی، پایان‌نامه کارشناسی ارشد حقوق خصوصی، دانشگاه تربیت مدرس، ۱۳۸۷
۵. هیأت مؤلفان انتشارات میکروسافت، فرهنگ تشریحی اصطلاحات کامپیوتری میکروسافت، ترجمه فرهاد قلی‌زاده نوری، چ٤، انتشارات آذرباد، ۱۳۷۹.
6. Federal Financial Institution Examination Council, information security, aa:http://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf,2006.
7. Henry Wolfe," Forensics and the Emerging Importance Evidence Gathering",aa:http://nzcs.org.nz/sITE-Default/x-files/4915pdf, 2001.
8. Sudhanshu Kairab, A Practical Guide to Security Assessments, CRC Press Company, London , 2004.
9. United National, Convention On The Use Of Electronic Communications In International Contract 2007, www.uncitral.org.
10. United National, UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, 1996, United National. www.Uncitral.org/pdf/English/texts/electoms/ml-ecommon.html.
11. University of California Business and Finance Bulletin,"IS-3 Electronic Information Security", 2008. http://people.seas.harvard.edu/~tmoore/science-econ.pdf

JOURNAL OF

LEGAL RESEARCH

VOL. VIII, No. 2 2009-2

Articles

- Access to Legal Assistance in Police Investigations
- The Right of Buyer for Deficiencies of Goods
- Civil Responsibility Concerning Natural Incidents
- Revocation of Labor Contract according to the Law of Iran
- The Extra-territoriality of the International Covenant on Civil and Political Rights
- Secured Information System in Electronic Commerce Law
- Contradictory Approaches to the Right of Self Determination
- Some Considerations on the Constitutional Council of the French Republic
- "Fair and Just" Treatment of the Host State concerning the Foreign Investment Contracts
- Compensation for the Breach of Foreign Investment Contracts
- The UN International Law Commission and the Common Natural Resources

Special Issue: Oil and Gas Law in National and International Systems

- The Companionship of the Energy Sector and WTO Regulations: Facts, Challenges and Prospects
- Stabilization Clause in the Sample Contracts of Detection and Derivation of Petroleum
- Oil Companies in Iran and the Problem of Diplomatic Protection
- Private Ownership in the Case of Oil and Gas Resources under the USA Law
- Investment Dispute Settlement in Energy Charter Treaty (ECT) and Legal effects of Iran's Accession thereto

Critique and Presentation

- A Critical Analysis of 'The Procedure Act of the Administrative Court of Justice'
- Some Critics on the Parliament's Draft Concerning Change of the UN's Headquarter
- Copenhagen Conference (2009) and Combating the Climate Change

ISSN: 1682-9220

S. D. I. L.
The S.D. Institute of Law
Research & Study