تحلیل حقوقی جنبه‌های ثبوتی و اثباتی انتساب داده پیام در قانون تجارت الکترونیک ایران

پرویز ساورایی*

تاریخ دریافت: ۹۹/۰۵/۱۱ تاریخ پذیرش: ۹۹/۱۰/۱۲

چکیده

«انتساب داده پیام» یکی از مهم‌ترین موضوعات قانون تجارت الکترونیک ایران است. به دلیل جدید بودن موضوع و ضعیف بودن ادبیات حقوقی و فنی مربوط، ممکن است درک و تفسیر صحیحی از قانون به عمل نیاید. در این مقاله کوشش می‌شود تا ضمن تحلیل مواد ۱۸ تا ۲۱ قانون تجارت الکترونیک ایران و ارائهٔ پیشنهاد در مورد اصلاح مفاد مادهٔ ۱۹، ابهامات مربوط به آنها نیز رفع گردد. مفهوم دقیق، عناصر، جنبه‌های ثبوتی و اثباتی« انتساب داده پیام»، روش‌های مطرح در اثبات انتساب، مفهوم و مصادیق شخص ثالث که در بند (ب) مادهٔ ۱۹ مستتر و به نحو بسیار مبهمی در قانون آمده است، مورد تجزیه و تحلیل و بحث قرار گرفته است. جنبه‌های اثباتی انتساب دادهٔ پیام در سه فرض، یعنی روش معرفی، توافقی و اقدامات شخص ثالث مطرح و تفسیر گردیده است. مباحث مهم دیگری چون روش‌های مطمئن و عادی و رویهٔ ایمن در انتساب داده پیام مورد بحث قرار گرفته است: رویهٔ ایمن و اقسام آن در انتساب دادهٔ پیام از لحاظ فنی ممکن است خیلی پیچیده باشد؛ مانند سیستم رمزنگاری نامتقارن (استفاده از کلید عمومی و خصوصی) و یا ساده باشد؛ مانند تأیید هویت ارسال‌کننده از طریق خط تلفن.

کلیدواژگان:

انتساب داده پیام، جنبه‌های ثبوتی و اثباتی، رویه ایمن.

* دانشیار دانشکده حقوق، دانشگاه شهید بهشتی.

savrai@iran-attorney.com &p-savrai@sbu.ac.ir

مقدمه

پیشرفت فناوری اطلاعات و فراگیر شدن ارتباطات الکترونیک، به‌خصوص در امر تجارت، منجر به افزایش روابط حقوقی میان اشخاص گردیده و در نتیجه نظام‌های حقوقی دنیا را با انبوهی از مشکلات حقوقی مواجه کرده است. در این میان، «انتساب داده پیام» به اصل ساز به یکی از مهم‌ترین موضوعات حقوقی در فضای مجازی تبدیل شده است. وجود پرسش‌های متعدد در این خصوص و نیز کمبود منابع در این زمینه، انگیزه‌ای شد که نسبت به رفع ابهامات و درک بهتر مقررات قانون تجارت الکترونیک،[1] پژوهشی به عمل آید.

در مبحث اول، تحت عنوان شناخت انتساب داده پیام، پرسش‌هایی چون مفهوم دقیق و عناصر«انتساب داده پیام» و این که چرا مقنن مقررات اصلی «انتساب داده پیام» را در دو مادهٔ مهم، یعنی مواد ۱۸ و ۱۹، مطرح کرده و اساساً فلسفهٔ وجودی وضع مقررات در این دو ماده چه بوده است، بررسی نموده و پاسخ آنها را در قالب قانون‌گذاری در دو جنبهٔ ثبوتی و اثباتی داده پیام داده‌ایم.

در مبحث دوم، جنبه‌های ثبوتی انتساب داده پیام و اشکالات شکلی و ترجمه‌ای مادهٔ ۱۹ مطرح و پیشنهاداتی به منظور اصلاح مفاد این ماده ارائه گردیده است.

در مبحث سوم، تحت عنوان جنبه‌های اثباتی انتساب داده پیام، این پرسش‌ها مطرح شده است: اولاً، روش‌های حقوقی انتساب داده پیام به چه طرقی است؟ ثانیاً، طرق فنی انتساب داده پیام با چه روش‌هایی محقق می‌گردد؟ در این راستا، مباحث مهمی چون روش‌های مطمئن، عادی و رویهٔ ایمن در انتساب داده پیام مورد بحث قرار گرفته و در نهایت مفهوم و مصادیق شخص ثالث را که در بند (ب) ماده ۱۹ مستتر و به نحو بسیار مبهمی در قانون آمده است، مورد تجزیه و تحلیل و بحث قرارداده‌ایم.

---

۱. عبارت «قانون تجارت الکترونیک» به صورت «قانون تجارت الکترونیکی» نیز شنیده و خوانده می‌شود. برای هر فردی این سوال مطرح می‌گردد که کدام عبارت صحیح است؟ در پاسخ باید گفت که عبارت «قانون تجارت الکترونیک» صحیح است. دلیل این امر آن است که خود کلمهٔ «تجارت» اسم است و کلمه بعدی آن باید به صورت صفت آورده شود. کلمه "Electronic" در زبان انگلیسی صفت است و اسم آن یعنی "Electron" با اضافه شدن پسوند "ic" به صفت تبدیل می‌شود؛ لذا به هنگام اضافه کردن آن به کلمه «تجارت» که اسم است؛ دیگر نیازی نیست «ی» نسبت را به آن اضافه کنیم.

۱. شناخت انتساب داده پیام

۱.۱. مفهوم انتساب داده پیام و عناصر آن

انتساب در مفهوم لغوی به معنی نسبت دادن، ارتباط، پیوستگی و وابستگی است.[۱] در زبان انگلیسی واژهٔ انتساب[۲] به معنای «باور به اینکه چیزی نتیجهٔ چیز دیگری است» و «باور به اینکه کسی مسئول چیزی است».[۳] اما خود عبارت «انتساب داده پیام»[۴] در معنای لغوی به معنی تعیین منبع داده پیام است؛ یعنی مؤلف یا خالق دادهٔ پیام چه شخصی است و یا اینکه منبع اصلی آن چیست.[۵]

مفهوم حقوقی انتساب داده پیام از مفهوم لغوی آن دور نیست. خود کلمهٔ «انتساب» به معنای تعلق امری به فرد خاصی است.[۶] در همین راستا می‌توان بیان داشت که انتساب داده پیام به معنای تعلق داده پیام به فرد معینی است؛ مثلاً انتساب یک سند یا امضای الکترونیک به یک شخص معین[۷] مشروط بر اینکه ناشی از اقدامات آن شخص و یا فرد باشد.[۸] به عبارت دیگر، آفرینش یا ارسال داده پیام از سوی منبعی که هویت دارندهٔ آن منبع تأیید[۹] و ارسال آن توسط وی تصدیق (احراز هویت)[۱۰] گردیده است، انتساب محسوب خواهد شد. با توجه به تعاریف یادشده، انتساب داده پیام واجد سه عنصر به شرح زیر است:

- آفرینش داده پیام و یا ارسال داده پیام،
- تأیید هویت دارنده منبع آفرینش داده پیام و یا ارسال‌کنندهٔ داده پیام،

---

۱. لغت نامه اینترنتی دهخدا و فرهنگ معین.

2. Attribution
3. Oxford Advance Learners Online Dictionary.
4. Attribution of Data Message
5. Merriam-Webster (https://www.merriam-webster.com/dictionary/attribution), Accessed 24 Oct. 2020.
6. Anjanette, H., Raymond & J., Benjamin, Lambert in "Technology, E-commerce and the Emerging Harmonization: the Growing Body of International Instruments Facilitating Ecommerce and the Continuing Need to Encourage Wide Adoption", (2014) 17 *International Trade and Business Law Review* 419 at 432.
7. Loc. Cit.
8. Manuel, Alba, "Order out of Chaos: Technology, Intermediation, Trust, and Reliability as the Basis for the Recognition of Legal Effects in Electronic Transactions", *Creighton Law Review,* Vol. 47, 2014, 387 at 390-391; National Conference of Commissioners on Uniform State Laws, *Uniform Electronic Transactions Act* (1999) Drafted by the National Conference of Commissioners on Uniform State Laws (with Prefatory Note and Comments) (Hereinafter *UETA*), 1999, Section 9.
9. Authentication
10. Identification

- احراز هویت خالق و یا ارسال‌کنندهٔ داده پیام.

باید توجه داشته باشیم که مفهوم «انتساب» "Attribution"با مفهوم «تأیید هویت» "Authentication" دارندهٔ منبع داده پیام در فضای مجازی یکی تلقی نگردد؛ این الفاظ دو مقوله متفاوت از یکدیگرند.[1] «تأیید هویت» دارندهٔ منبع داده پیام از عناصر انتساب محسوب می‌گردد. انتساب به این امر مربوط می‌شود که آیا می‌توان داده پیام را به یک شخص معین ارتباط داد یا خیر و اینکه آیا داده پیام واقعاً به وسیلهٔ نامبرده ارسال گردیده است یا خیر.[2] در صورت احراز انتساب، کاربر مسئول داده پیام ارسالی است. باید توجه شود که وجود امضای الکترونیک که حاکی از تأیید هویت امضاءکننده باشد، الزاماً به این معنا نخواهد بود که داده پیام به وی منتسب گردد؛[3] چرا که ممکن است مثلاً شخصی از طریق نفوذ به حساب کاربری شخص دیگری، پیام را ارسال کرده باشد و یا اینکه به هنگام ارسال، جنونی حادث شده باشد و در اینجا است که تفاوت "Attribution" و "Authentication" آشکار می‌گردد.

به همین ترتیب، «انتساب» را نباید با «احراز هویت» "Identification" در فضای مجازی اشتباه کرد. احراز هویت به تأیید شخص امضاءکننده مربوط می‌شود؛ یعنی آیا امضاءکننده همان فردی است که خود را معرفی کرده است؟ در حالی‌که انتساب به این امر مربوط می‌گردد که آیا می‌توان داده پیام را به یک شخص معین منتسب کرد یا خیر؛ مثلاً انتساب در متن یک سند مربوط می‌شود به این امر که آیا امضای مندرج در آن ناشی از عمل یک شخص معین است یا خیر؛ در حالی‌که احراز هویت مربوط می‌شود به تأیید شخص امضاءکننده؛ یعنی آیا همان فردی است که خود را معرفی کرده یا خیر. در اینجا، احراز هویت به مثابه تأیید هویت متعلق به کسی تعریف می‌گردد؛[4] مثلاً «الف» به عنوان یک طرف متکی به صحت یک ابزار نوشتاری، می‌خواهد بداند که هویت امضاءکننده تأیید شده و وی واقعاً سند را امضاء کرده است یا خیر . در خصوص

1. Randolph, A., Kahn & Dianne J., Silverberg, "From Mount Sinai to Cyberspace: Making Good E-business Records", *Business Lawyer*, Vol. 57, 2001, 431 at 432.
2. Tana, Pistorius, "Nobody Knows You're a Dog: The Attribution of Data Messages", *South African Mercantile Law Journal*, Volume 14, 2002, 737 at 739; Manuel, Alba, Op. Cit.
3. Jason, Mikellyn, Charles, Johnson, Transactions of the Centre for Business Law, "*Consequences of and Problems with Electronic Contracts*", University of the Free State, Chapter 8, Issue 37, 2005, pp. 89 – 129.
4. Schellekens, MHM., *Electronic Signatures: Authentication Technology from a Legal Perspective*, TMC Asser Press, The Hague The Netherlands, 2004, at 59; Andrej, Savin, *EU Internet Law, Elgar European law*, Edward Elgar Pub., 2013, at 219.

انتساب داده پیام در ابتدا احراز هویت می‌شود و سپس اقدامات شخصی که احراز هویت گردیده به آن سند نسبت داده می‌شود؛ یعنی احراز هویت همیشه اولین قدم است، سپس انتساب سند به وی. به طور خلاصه، در ارسال داده پیام، ابتدا تشخیص هویت دارندهٔ منبع داده پیام مشخص می‌شود و سپس احراز هویت و در نهایت انتساب محقق می‌گردد.

۱.۲. قانون‌گذاری در دو جنبه ثبوتی و اثباتی داده پیام

در خصوص مواد ۱۸ و ۱۹ که تا حدود زیادی از مقررات نمونهٔ آنسیترال برای تجارت الکترونیک[1] اقتباس شده، ممکن است این پرسش مطرح گردد که چه تفاوتی میان مواد مذکور وجود دارد و اساساً فلسفه و هدف مقنن از وضع این مواد چه بوده است؟

برای پاسخ به پرسش مذکور و فهم بهتر این دو مواد، در ابتدا باید به طور مختصر به توضیح مقوله‌های «ثبوت» و «اثبات» در علم حقوق پرداخت. اثبات در مقابل ثبوت قرار دارد.[2] بر همین مبنا، نهادهای حقوقی را به دو مرحلهٔ ثبوت و اثبات تقسیم می‌کنند؛ مثلاً وجود هر حقی، مرحلهٔ ثبوت آن است و اثبات آن مشخص می‌کند که چه شخصی ذی‌حق است.[3] در همین ارتباط نیز مادهٔ ۱۸ جنبهٔ ثبوتی داده پیام و مادهٔ ۱۹ جنبهٔ اثباتی آن را مد نظر قرار داده است.

۲. جنبه‌های ثبوتی انتساب داده پیام و اشکالات شکلی و ترجمه‌ای مادهٔ ۱۹ و اصلاح آن

۱.۲. جنبه‌های ثبوتی انتساب داده پیام

به دلیل ماهیت الکترونیک داده پیام، قابلیت انتساب آن به فرد معین در فضای مجازی به سهولت قابلیت انتساب اسناد کاغذی نیست. انتساب در اسناد کاغذی به فرد معین را می‌توان از طریق مراجعه به کارشناس خط و امضاء و دلایل دیگر محقق ساخت؛ ولی انتساب اسناد

1. United Nations, *United Nations Uncitral Model Law on Electronic Commerce Guide to Enactment*, United Nations Publications, 1996 with additional article 5 as adopted in 1998", Article 13 (Hereinafter *UNCITRAL Model Law*).

۲. جعفری لنگرودی، محمد جعفر، ***دانش نامه حقوقی***، موسسه انتشارات امیرکبیر، چاپ پنجم، ص ۸۰۶.

۳. جعفری لنگرودی، محمدجعفر، ***دوره پنج جلدی مبسوط در ترمینولوژی حقوق***، جلد ۱، شماره ۳۹۰، گنج دانش.

الکترونیک حتی با وجود امضاء ممکن است بسیار دشوار باشد؛ چرا کـه در فضـای مجـازی ایـن امکان وجود دارد که فردی به‌طور غیر مجاز با به دست آوردن رمز عبور یا کدهای تصدیق مربوط به شخص دیگر، داده پیامی را ارسال و یا پست کرده باشد[1] و این امر در حالی می‌تواند محقق گردد که احراز هویت از طریق کدگذاری، رمزگذاری و یا موارد مشابه به طور صـحیح واقـع شـده باشـد.[2] ظاهر این وضعیت نشان می‌دهد که داده پیام توسط شخصی که هویتش تصـدیق گردیـده، ارسـال شده، اما در حقیقت از سوی وی نبوده است. با توجه به مشکل یادشده و نیز حل نسبی آن، ماده ۱۸ قانون تجارت الکترونیک ایران در جنبه ثبوتی انتساب داده پیام، چنین مقرر می‌دارد:

«در موارد زیر داده پیام منسوب به اصل ساز است:

الف) اگر توسط اصل ساز یا به وسیله شخصی ارسال شده باشد که از جانب اصل سـاز مجـاز بـه این کار بوده است.[3]

ب) اگر به وسیلهٔ سیستم اطلاعاتی برنامه ریزی شده یا تصدی خودکار از جانب اصل ساز ارسـال شود».

قبل از تحلیل مادهٔ مذکور، باید اذعان داشت کـه نقـص مقـررات مـادهٔ ۱۳ آنسـیترال بـرای تجارت الکترونیک و به تبع آن مادهٔ ۱۸ در این است که صرفاً «ارسال» داده پیام را بیان داشته و در مورد «تولید» یا «خلق یا آفرینش» داده پیام سکوت کرده‌اند. بنابراین، پرسشی کـه در اینجـا مطرح می‌شود، این است که چنانچه داده پیامی تولید شود، ولی ارسال نگـردد، انتسـاب بـه چـه صورت محقق می‌گردد؟

در پاسخ به پرسش یادشده می‌توان از عمومات مواد مذکور در این قانون، این نتیجه را گرفت که احکام انتساب در مورد ارسال، دربارهٔ تولید داده پیام نیز جاری و ساری است. به‌عـلاوه، وقتـی مقنن ارسال داده پیام از سوی اصل ساز را منتسب به وی می‌داند، به طریق اولـی داده پیـامی را که توسط او تولید و یا خلق می‌گردد، نیز منتسب به وی تلقی می‌کنـد. بنـد (ب) مـاده ۲ قـانون

1. Article 13. Attribution of data messages, *UNCITRAL Model Law*, Note 83, p. 49.
2. United Nations Commission on International Trade Law, *Promoting Confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods,* United Nations, Vienna, 2009, Note 99, P. 44.
3. See also *UETA,* Section 9 (a), 1999. Available at:
https://www.uniformlaws.org/viewdocument/final-act-no-comments-27?CommunityKey=2c04b76c-2b7d-4399-977e-d5876ba7e034&tab=librarydocuments
Australian Electronic Transactions Act 1999, Section 15 (1). Available at:
http://www.comlaw.gov.au/Details/C2011C00445/Html/Text#_Toc296406974

تجارت الکترونیک که در تعریف اصل ساز مقرر می‌دارد: «اصل ساز منشأ اصلی داده پیام است که داده پیام به وسیله او یا از طرف او تولید یا ارسال می‌شود»؛ لفظ «تولید» را که به معنی «خلق و یا آفرینش» است، در کنار لفظ «ارسال» مورد استفاده قرار داده است.

مفاد مادۀ ۱۸ در جایی به کار می‌رود که داده پیام واقعاً به وسیله اصل ساز ارسال شده باشد. هدف از تأسیس مقررات این ماده، بیان فرضی است که انتساب داده پیام تحت شرایط خاصی، منتسب به اصل ساز یا نمایندۀ او تلقی گردد. مادۀ ۱۸ درصدد انتساب داده پیام و تعیین و احراز هویت شخص خاصی نیست. در این فرض، اصل بر این است که ارسال‌کننده داده پیام مسئول داده پیام ارسالی است؛ در صورتی‌که واقعاً از سوی وی ارسال شده باشد.[1]

قسمت دوم بند (الف) مادۀ ۱۸ به شرایطی اطلاق می‌شود که داده پیام توسط شخصی غیر از اصل ساز، یعنی نمایندۀ وی (مثلاً وکیل و یا منشی) که اختیار اقدام از طرف نامبرده را صراحتاً یا ضمناً[2] دارد، ارسال شده باشد. طبق مقررات آنسیترال، اینکه نماینده چه شخصی است، بستگی به تعریف آن در حقوق داخلی کشورها دارد.[3] در هر حال، در وضعیت یادشده، داده پیام منسوب به ارسال‌کننده تلقی خواهد شد. بند (ب) مادۀ ۱۸ نیز قاعده‌ای را مقرر می‌دارد که داده پیام، اگر به وسیله سیستم اطلاعاتی برنامه‌ریزی شده یا تصدی خودکار از جانب اصل ساز ارسال شود، منسوب به اصل ساز تلقی خواهد شد.[4]

در کلیه شقوق فوق، فرض بر این است که داده پیام از سوی اصل ساز ارسال شده باشد؛ مگر آنکه خلاف آن ثابت شود. پرسشی که در اینجا مطرح می‌شود، این است که در صورت انکار انتساب، بار اثبات به عهدۀ چه شخصی است؟

مقررات قانون تجارت الکترونیک ایران و آنسیترال در این خصوص ساکت‌اند؛ لذا به استناد قاعدۀ سنتی مبنی بر اینکه «مدعی باید ادعای خود را ثابت کند»، در دنیای الکترونیک نیز

1. United Nations Commission on International Trade Law, Op. Cit; Article 13, *UNCITRAL Model Law,* Notes 83, 84, 99 & 100, P. 44.
2. Phang, A., & Seng D., "The Singapore Electronic Transactions Act 1998 and the Proposed Article 2B of the Uniform Commercial Code" *International Journal of Law and Information Technology*, Volume 7, 1999, p. 110.
3. United Nations Commission on International Trade Law, Op. Cit; *UNCITRAL Model Law*, Note 84.
4. Phang, A., & Seng, D., Op. Cit.

چنانچه شخصی ادعا کند که داده پیام منتسب به شخص معینی است، در این صورت بار اثبات به عهدهٔ وی خواهد بود.[1]

۲.۲. اشکالات شکلی و ترجمه‌ای مادهٔ ۱۹ و اصلاح آن

«داده پیامی که بر اساس یکی از شروط زیر ارسال می شود، مخاطب حق دارد آن را ارسال شده محسوب کرده و مطابق چنین فرضی (ارسال شده) عمل نماید:

الف) قبلاً به وسیلهٔ اصل ساز روشی معرفی و یا توافق شده باشد که معلوم کند آیا داده پیام همان است که اصل ساز ارسال کرده است.

ب) داده پیام دریافت شده توسط مخاطب از اقدامات شخصی ناشی شده که رابطه اش با اصل ساز، یا نمایندگان وی باعث شده تا شخص مذکور به روش مورد استفاده اصل ساز دسترسی یافته و داده پیام را به مثابه داده پیام خود بشناسد».

مادهٔ ۱۹ یادشده دارای اشکالات زیر است:

برای گویاتر کردن صدر این ماده، می‌توان به جای کلمهٔ «شروط» از کلمهٔ «فروض» استفاده کرد: واژه «شروط» در مادهٔ یادشده هرگز دلالتی بر شرط به معنای متعارف کلمه ندارد؛ بلکه ناظر بر چند فرض است که داده پیام در صورت مطابقت با آنها مشمول حکم مندرج در ماده خواهد بود. بنابراین، می‌توان به جای واژهٔ «شروط» از واژه «فروض» یا «روش‌ها» استفاده کرد.

الزامی به ذکر الفاظ «ارسال شده» نیز وجود ندارد.

ایراد دیگر مربوط به بند (الف) مادهٔ مذکور است که در آن از واژهٔ «آیا» استفاده شده که به وضوح حشو و زائد است و مسلماً با حذف آن، معنا با صراحت و بلاغت بیشتری ابراز می‌گردد. معلوم نیست چرا قانون‌گذار این بند را به صورت جملهٔ پرسشی آورده است. اساساً، عبارت قانون به صورت سؤالی آورده نمی‌شود و وجود کلمهٔ «آیا» فهم قانون را با ابهام و تردید مواجه می‌سازد. در مقام قانون‌گذاری و در فارسی روان، نیازی به آوردن کلمهٔ «آیا» نیست. به‌علاوه، قانون‌گذار احکام وضعی وضع می‌کند؛ به عبارت دیگر، احکام قانون عموماً بایدها و نبایدهاست و در این راستا عموماً از الفاظ استفهامی و پرسشی که مبین وضع حکمی نباشند، نباید استفاده کرد.

1. Boss, Amelia, H., "Searching for Security in the Law of Electronic Commerce", *Nova Law Review*, Volume 23, Issue 2, 1999, P. 612.

نکتهٔ ابهام‌آمیز دیگری که در بند (ب) این ماده به چشم می‌خورد، این است که مرجع ضمیر کلمهٔ «خود» کیست؟ معلوم نیست که این کلمه به چه کسی عطف می‌شود. علت این ابهام ترجمهٔ تحت‌اللفظی مفاد بند (ب) مادهٔ ۱۹ است. آنچه که از مفاد بند (ب) استنباط می‌گردد، این است که در خصوص موضوع انتساب، شخص دیگری غیر از اصل ساز و مخاطب نیز حضور دارد؛ لذا برای فهم بهتر این بند، اگر به جای کلمهٔ «شخصی» از کلمهٔ «ثالثی» استفاده گردد، منظور مقنن به راحتی قابل درک خواهد بود. بر همین اساس و نیز با توجه به ایرادات نگارشی مادهٔ ۱۹ و در نهایت برای درک و تحلیل حقوقی بهتر این ماده، بند (ب) آن را به شرح زیر اصلاح می‌کنیم:

«داده پیامی که مخاطب دریافت می‌کند، از اقدامات ثالثی ناشی شده که به علت رابطه‌اش با اصل ساز یا نمایندهٔ اصل ساز توانسته به روش مورد استفاده اصل ساز دسترسی پیدا کند و داده پیامش به مثابه داده پیام اصل ساز است».

۳. جنبه‌های اثباتی انتساب داده پیام

ماده ۱۹ سه فرض معرفی، توافق و اقدامات شخص ثالث را برای اثبات انتساب داده پیام بیان داشته است.

۳.۱. روش معرفی و توافقی

در فرض معرفی، اصل ساز برای پذیرش الزامات خود به طور یکجانبه، روشی را معرفی می‌کند که به واسطهٔ آن اگر مخاطب داده پیامی از وی دریافت نماید، به معنای ارسال و پذیرش محتوای داده پیام از سوی اصل ساز تلقی می‌شود؛ مانند معرفی یک سایت اینترنتی یا وبلاگ یا ایمیل یا غیره. در روش توافقی، روش مورد نظر یا روند شناسایی، مورد توافق طرفین قرار می‌گیرد؛ مثلاً در قرارداد فیمابین، روش یا روش‌های ارتباطی را مشخص می‌کنند: ارسال داده پیام از طریق فاکس، ایمیل و غیره. به موجب پاراگراف a ۳ مادهٔ ۱۳ مقررات آنسیترال که بند (الف) مادهٔ ۱۹ از آن اقتباس یافته است، اگر مخاطب فرایند تعیین هویت مورد توافق قبلی را که با اصل ساز کرده، به آن عمل نماید، در این صورت، فرض بر این است پیام مربوط به اصل ساز است. این وضعیت نه تنها شامل وضعیت فرایند تعیین هویت مورد توافق بین اصل ساز و مخاطب می‌شود، بلکه همچنین شامل وضعیتی نیز می‌گردد که اصل ساز یکطرفه یا در نتیجهٔ

توافق با یک واسطه، روشی را مشخص کرده باشد و بدین طریق خود را بـه داده پیـامی ملـزم و مقید کند که طبق شرایط روش مزبور ارسال گردیده است. بنابراین، توافقـاتی کـه نـه از طریـق توافق مستقیم فیمابین اصل ساز و مخاطب، بلکه از طریـق دخالـت شـخص ثالـث ارائـه‌دهنـده خدمات محقق می‌شود، مشمول پاراگراف a ۳ (بند الف مادهٔ ۱۹) می‌گردند.[1]

روش تصدیقی، موضوع مواد ۲۲ و ۲۳ قانون تجارت الکترونیـک نیـز نـوع دیگـری از روش توافقی محسوب می‌گردد. روش تصدیقی یکی از روش‌های مختلف تأمین امنیـت در مبادلـهٔ داده پیام است که هم برای تصدیق انتساب داده پیام به اصل ساز و هم برای تصدیق هویت اصل ساز به کار می‌روند و خود دارای مصادیق متفاوت به شرح مندرج در مواد مذکور است.

نکتهٔ مهم مذکور در در بند (الف) مادهٔ 19 کلمه «روش» است که بـه صـورت عـام تصـریح گردیده است؛ بنابراین، این روش می‌تواند به صورت عادی یا مطمئن باشد.

۳.۱.۱. روش عادی

در روش عادی، شخص با معرفی روش مورد نظر به مخاطبین بالقوه خود اعلام می‌کنـد کـه در صورت دریافت داده پیام از طریق روش معرفی شـده، داده پیـام منتسـب بـه او تلقـی گـردد. روش‌های معرفی به دو صورت محقق می‌شوند: مستقیم و غیر مستقیم؛ مثلاً شخص «الـف» بـا دادن کارت ویزیت خود که حـاوی شـماره تلفـن، وب‌سـایت و آدرس ایمیـل اسـت، روش‌هـای ارتباطی را به مخاطب معرفی می‌کند. بنابراین، وقتی مخاطب ایمیلی از طریق روش معرفی شده شخص «الف» دریافت می‌کند، فرض بر این است که از سوی شخص «الف» ارسال شده اسـت یا مثلاً شرکت سونی در سایت خود صفحه شبکه‌های ارتباط مجازی را به نام راه ارتبـاطی خـود معرفی می‌نماید؛ فلذا هرگونه داده پیام دریافتی از روش‌های معرفی شده منتسب به سونی خواهد بود. در روش غیرمستقیم، اصل ساز روش خود را اعلام نمی‌کنـد، ولـیکن بـه طـور ضـمنی داده پیام‌های ارسالی را منتسب به خود می‌داند؛ مثلاً دارندهٔ نام دامنه‌ای که بر اساس نام دامنه، ایمیل یا ایمیل‌هایی برای خود ساخته است، هرگونه ایمیل دریـافتی از آن نـام دامنـه منسـوب بـه وی خواهد شد. در مورد مالک شماره تلفن همراه، فرض بر این است که در قبال پیامـک‌هـای هـای ارسالی مسئول تلقی می‌شود. ایمیل‌هایی که افراد از شرکت‌های مختلف به طور مجـانی دریافـت

1. *UNCITRAL Model Law*, Comments, Note 86.

می‌دارند، فرض بر این است که این افراد در قبال ایمیل‌های ارسالی مسئول تلقی می‌شوند. استفادهٔ مکرر از یک ایمیل با نام مشخص، مبین این امر است که شخص مزبور از این ایمیل به طور متعارف استفاده می‌کند که در صورت تأیید هویت دارندهٔ منبع داده پیام، احراز هویت شخص و عمل انتساب کار دشواری نخواهد بود.

استفاده از روش‌های عادی ارسال پیام در عصر حاضر فوق‌العاده زیاد است و از لحاظ حجم، قابل مقایسه با روش مطمئن نیست و بسیاری از دعاوی و اختلافات مربوط به همین روش‌های عادی است؛ مثلاً پست الکترونیک و پیام‌های الکترونیک[1] ابزار اصلی در ارتباطات بین اشخاص شده است و هیچ شکلی از اطلاعات ذخیره شدهٔ الکترونیک را نمی‌توان یافت که فراگیرتر از پست و پیام‌های الکترونیک باشد. در سیستم قضایی آمریکا کمتر دعاوی به چشم می‌خورند که عموماً به نوعی با پیام الکترونیک ارتباط نداشته باشند.[2] دادگاه‌های آمریکا[3] و نیز قوانین بسیاری از کشورها[4] در ارتباط با پذیرش انتساب در موارد بالا انعطاف زیادی به خرج داده‌اند. با این حال، روش‌های عادی ارسال پیام مشکلات مهم حقوقی را در خصوص انتساب داده پیام، نیز مطرح کرده است. دخل و تصرف در آن مشکل نیست و به آسانی قابل تغییر است. استفاده از آن ارزان و در دسترس هر کسی است و مهم‌تر از همه اینکه کشف یک چنین دخل و تصرفاتی در بسیاری از موارد غیر ممکن است. مسئلهٔ دیگری که در همین خصوص مطرح می‌شود، اسناد ضمیمهٔ پست الکترونیک است: تهیه‌کنندهٔ آن ممکن است شخص ثالث باشد، نه اصل ساز. مشکل انتساب داده پیام در مورد افرادی که از شبکه‌های اجتماعی مانند تلگرام، واتس‌اپ و سیگنال که از سیستم رمزگذاری پایانه به پایانه[5] استفاده می‌کنند، دو چندان می‌شود. چنین مشکلاتی اهمیت عناصر تشخیص هویت دارندهٔ منبع داده پیام، احراز هویت ارسال‌کننده و

1. Electronic Mails and Text Messages
2. See *Lorraine v. Markel Am. Ins. Co*., 241 F.R.D. 534, 554 (D. Md. 2007).
3. *Commonwealth Aluminum Corporation v. Stanley Metal Associates*, United States District Court for the Western District of Kentucky, 9 August 2001, Federal Supplement, 2nd series, vol. 186, p. 770; and *Central Illinois Light Company (CILCO) v. Consolidation Coal Company (Consol)*, United States District Court for the Central District of Illinois, 30 December 2002, Federal Supplement, 2nd series, vol. 235, p. 916; *Sea-Land Service, Inc. v. Lozen International, LLC*, United States Court of Appeals for the Ninth Circuit, 3 April 2002, Federal Reporter, 3rd series, vol. 285, p. 808; *Superhighway Consulting, Inc. v. Techwave, Inc*., United States District Court for the Northern District of Illinois, Eastern Division, 16 November 1999, U.S. Dist. LEXIS 17910.
4. Agri, Repss, and Ilze, Znotina, "Electronic Evidence in Latvia: A General Overview", *Digital Evidence and Electronic Signature Law Review*, Volume Eight, 2100, P. 63.
5. End to End Encryption

یکپارچگی داده پیام و صحت محتوای آن و کنترل و یـا نظـارت مناسـب قضـایی را چنـد برابـر می‌کند؛ لذا وجدان مرجع قضایی به صرف تقدیم فرمت‌های کامپیوتری که متضمن یـک چنـین اطلاعاتی است، به راحتی اقناع نخواهد شد.[1] به هر حال، یک چنین سندی به عنوان دلیل مـورد پذیرش دادگاه قرار می‌گیرد؛ مشروط بر اینکه دارندهٔ یک چنین سـندی بتوانـد در صـورت انکـار طرف مقابل، انشا و ارسال آن از طرف ارسال‌کننده را اثبات نماید. در دعـوای Talada v. City of Martinez[2] محتویات و ارسال یک نامهٔ الکترونیک از طریق ادای شـهادت و نیـز پیـام‌هـای الکترونیک دیگر، به عنوان دلیل به نحو صحیح مـورد تأییـد و پـذیرش دادگـاه قـرار گرفـت. در دعـوای People v. Brown[3]، دادگـاه کالیفرنیـا در رأی خـود، اصـالت پیـام‌هـای الکترونیـک ارسال‌شده از سوی خوانده را به استناد شهادت شاهد را مبنی بر اینکه پیام‌ها از سوی متهم ارسال و در انتها با نام متهم امضا گردیده است، مورد تأیید قرار می‌دهد.

در دعوای Dickens v. State[4]، دادگاه به موجب قانون مریلند و با توجه به اوضاع و احـوال و قرائن (از جمله یافتن تلفن همراه در محل نزدیک به خانه قربانی و اظهارات متهم نزد ساکنین مبنی بر این که اقدامی علیه همسرش انجام داده اسـت) و شـهادت مـادر قربـانی جـرم، ارسـال پیام‌های الکترونیک از طرف شوهر قربانی به همسرش و نیز محتویات پیـام‌هـای الکترونیـک را مورد تصدیق قرار داد.

در اثبات انتساب داده پیام، دادگاه می‌تواند با استفاده از افراد متخصص اینترنت، خدمات اینترنتی و و افراد متخصص دیگر در خصوص چگونگی ارسال و دریافت پیام‌های و اینکه چگونه یک چنـین پیام‌هایی ذخیره و احیا می‌گردند، برای تصدیق و انتساب داده پیام مورد استفاده قرار دهد.[5]

پرسش مهمی که در اینجا مطرح می‌گردد، این است که چگونه در مورد دارندهٔ ایمیلی که نام جعلی دارد، بتوان ایمیل مزبور را به وی منتسب کرد؟

مقایسهٔ پیام‌های الکترونیک موجود با دیگر پیام‌های الکترونیک که قـبلاً اصـالت آنهـا مـورد تصدیق قرار گرفته‌اند، می‌تواند در انتساب پیام‌های موجود مورد اسـتفاده قرارگیرنـد.[6] ایـن روش

1. Yun Zhao, *Dispute Resolution in Electronic Commerce*, Martinus Nijhoff Publishers, 2005, pp. 14 et sq.
2. 656 F. Supp. 2d 1147, 1158 (N.D. Cal. 2009).
3. A122791, 2009 WL 1878704, at *3 (Cal. Ct. App. June 30, 2009).
4. 927 A.2d 32, 36-37 (Md. Ct. Spec. App. 2007).
5. See *State v. Taylor*, 632 S.E.2d 218, 230 (N.C. Ct. App. 2006).
6. See *United States v. Safavian*, 435 F. Supp. 2d 36, 40 (D.D.C. 2006).

به‌طور خاص در مواردی مورد استفاده قرار می‌گیرد که آدرس پست الکترونیک ارسال‌کننده یا دریافت‌کننده فاقد نشانه هویتی باشد؛ برای مثال آدرس پست الکترونیک joe.smith@doj.gov مبین این امر است که این آدرس پستی متعلق به آقای اسمیت است که به احتمال زیاد در وزارت دادگستری شاغل است.[1]

آدرس پست الکترونیک MerrittDC@aol.com متضمن همان عناصر آشکار تشخیص هویت نیست، اما با مقایسه با محتویات پست الکترونیک اول که قبلاً هویت وی به نحو مستقل و صحیح مورد تصدیق قرار گرفته، می‌توان هویت ارسال‌کننده یا دریافت‌کنندهٔ پست الکترونیک دوم را نیز مورد تصدیق قرار داد.

۳.۱.۲. روش مطمئن

روش مطمئن یکی از مصادیق استفاده از رویهٔ ایمن است. استفاده از رویهٔ ایمن به منزلهٔ استفاده از ابزار فنی به منظور اثبات انتساب داده پیام به کار می‌رود. لازم به تأکید است که رویه‌های ایمن به معنای این امر نیست که سایر اشکال اثباتی انتساب به روش عادی به شرحی که داده شد، فاقد ارزش اقناعی هستند.

تعریف «رویه ایمن» طبق بند ۱۴ از مادهٔ ۲ مقررات متحدالشکل معاملات الکترونیک آمریکا ۱۹۹۹ تنظیمی توسط کنفرانس ملی کمیسیونرها در مورد قوانین متحدالشکل آمریکا و نیز قانون معاملات الکترونیک سنگاپور[2] که بسیار شبیه به تعریف «رویه ایمن» در قانون تجارت الکترونیک ایران است،[3] رویه‌ای است به منظور تأیید امضا، سابقه یا عملی که مربوط به یک شخص خاص باشد یا رویه‌ای برای کشف تغییرات یا اشتباهات مربوط به اطلاعات مندرج در سابقهٔ الکترونیک است. از لحاظ فنی، رویهٔ ایمن روشی است برای احراز هویت یک شخص یا تأیید صحت یک پیام. این واژه متضمن روشی است که مستلزم استفاده از الگوریتم‌ها یا سایر کدها، کلمات یا ارقام شناسایی، رمزنگاری یا تصدیق با پاسخ برگشت و سایر طرق تصدیق است. رویهٔ ایمن ممکن است بسیار ساده باشد؛ مانند تماس از طریق تلفن به منظور تأیید هویت فرستنده از طریق کانال دیگر ارتباطی. همچنین رویهٔ ایمن امکان دارد مثلاً متضمن استفاده از

1. Loc. Cit.
2. *UETA,* P. 10; Singapore's Electronic Transaction Act Revised 2011.
۳. بند (ط) ماده ۲ قانون تجارت الکترونیک.

نام دخترانه مادر یا از طریق شماره شناسایی شخصی باشد. «روش‌های تصدیقی»[۱] نیز عموماً از دیگر روش‌های مختلف و ساده در تأمین امنیت در مبادلهٔ داده پیام است که خود دارای مصادیق متفاوتی است که هم برای تصدیق انتساب داده پیام به اصل ساز و هم برای تصدیق هویت اصل ساز به کار می‌روند. از سوی دیگر، رویهٔ ایمن ممکن است خیلی پیچیده باشد؛[۲] مانند سیستم رمزنگاری نامتقارن.[۳] استفاده از عملیات رمزنگاری (استفاده از کلید خصوصی و کلید عمومی) یکی از مهم‌ترین رویه‌های ایمن محسوب می‌گردد. به گفتهٔ لنس رز، استفاده از تکنیک‌های رمزگذاری، اساساً به معنی بی‌اعتمادی کاربران به امنیت سیستم، بی‌اعتمادی به مالک یا اپراتور سیستم و مقامات اجرای قانون است.[۴] رمزهای دیجیتال، شماره‌های شناسایی و نیز ترکیب کلیدهای عمومی و خصوصی از ابزارهای مهم انتساب محسوب می‌شوند[۵]. مجدداً تأکید می‌گردد که استفاده از روش‌های ایمن به این معنا نیست که سایر اشکال دارای اثر اقناعی نیستند،[۶] بلکه ارزش اثباتی هریک از روش‌ها با توجه به روش‌های ایمنی به کار رفته مورد توجه قرار خواهند گرفت.[۷] در همین خصوص مادهٔ ۱۳ قانون تجارت الکترونیک چنین مقرر می‌دارد:

«به‌طور کلی، ارزش اثباتی داده‌پیام‌ها با توجه به عوامل مطمئنه از جمله تناسب روش‌های ایمنی به کار گرفته شده با موضوع و منظور مبادله داده‌پیام تعیین می‌شود».

در رمزنگاری کلید عمومی[۸] از یک جفت کلید عمومی و کلید خصوصی استفاده می‌گردد. در این رمزنگاری، داده پیام با کلید عمومی، قفل، یعنی رمزنگاری می‌شود و به مخاطب ارسال می‌گردد و مخاطب نیز با در دست داشتن کلید خصوصی (کلید متناظرش) پیام را رمزگشایی می‌کند. پس به این ترتیب می‌توان گفت که جفت کلید عمومی و خصوصی، اعداد یا کلماتی‌اند

۱. روش تصدیقی، موضوع مواد ۲۲ و ۲۳ قانون تجارت الکترونیک ایران.

2. Mann, Ronald J., Warren, Elizabeth: Westbrook, Jay Lawrence, *Comprehensive Commercial Law 2018: Statutory Supplement (Supplements)* Paperback, 2018, Wolters Kluwer, New York, p. 1098.

3. Asymmetric Cryptography

4. Rose, Lance, *Netlaw: Your Rights in the Online World*, Osborne Mc Graw-Hill, 1995, p 182.

5. United Nations Commission on International Trade Law, Op. Cit., Note 103, P. 46.

6. Loc. Cit., Note 100, P. 44.

7. See United States, Uniform Electronic Transactions Act (1999), Official Comments on Section 9.

8. Yaman, Akdeniz & Others, "Cryptography and Liberty: 'Can the Trusted Third Parties Be Trusted? A Critique of the Recent UK Proposals", *Journal of Information Technology*, Vol. 2, 1997).

که مربوط به شخص یا سازمان یا تشکیلات می‌باشند. کلید عمومی، برای اشخاصی که تصمیم به انتقال اطلاعات رمزشده دارند، قابل دسترسی خواهد بود و کلید خصوصی در اختیار مخاطب است و برای بازگشایی اطلاعاتی به کار می‌رود که به وسیلهٔ کلید عمومی رمزگذاری شده است.

در امضای الکترونیک مطمئن از امضای دیجیتال با استفاده از رمزنگاری استفاده می‌شود؛ بدین توضیح که ارسال‌کننده، داده پیام را با کلید خصوصی خود رمزنگاری می‌کند و مخاطب نیز با در دست داشتن کلید عمومی، داده پیام ارسال‌کننده را رمزگشایی می‌کند.[1] در این فرایند در ابتدا هویت دارندهٔ منبع داده پیام مشخص و سپس هویت وی احراز و در نهایت انتساب محقق می‌شود؛ زیرا داده پیام که با کلید خصوصی ارسال‌کننده رمزنگاری شده، فقط با کلید عمومی او که در دست مخاطب است، رمزگشایی می‌شود و بدین وسیله مخاطب اطمینان حاصل می‌کند که این پیام از سوی شخص مورد نظر ارسال شده و هویت و اعتبار آن داده پیام را با استفاده از کلید عمومی مربوطه مشخص می‌نماید. امضاهای دیجیتال نه تنها موجب ایجاد اعتبار برای امضاها در یک سامانه تبادل داده و اطلاعات می‌گردد، بلکه سندیت و اعتبار ویژه‌ای به یک سند، خصوصاً انواع انتقال اطلاعات، مانند داده‌های مالی و محرمانه می‌بخشند. برای مثال، فرض کنید که بانک ملی ایران قصد دارد دستور پرداخت معتنابهی از ارز خارجی را به یک بانک خارجی ارسال کند. دریافت‌کنندهٔ این دستور که بانک خارجی است، اگر شک و تردید کند که این پیام از طرف یک منبع مجاز ارسال شده است یا خیر، طبیعتاً از انجام دستور خودداری و در نتیجه مشکلاتی را در روابط مالی بین المللی ایجاد می‌کند. دریافت‌کنندهٔ دستور باید از چند فاکتور اطمینان حاصل کند تا پرداخت را انجام دهد: یکپارچگی داده پیام، درستی و صحت داده پیام، تشخیص هویت دارندهٔ منبع داده پیام و در نهایت احراز هویت. استفاده از امضای دیجیتال این اطمینان را به مخاطب می‌دهد.

برای اخذ امضای دیجیتال و تضمین احراز هویت امضاکننده، به مرجع ثالثی نیازمند است که بتواند احراز هویت امضاکنندهٔ دیجیتال را تضمین کند. دفاتر خدمات صدور گواهی امضای

1. Froomkin, A., Michael, "The Essential Role of Trusted Third Parties in Electronic Commerce", *Oregon Law Review*, Vol. 75, 1996, PP. 51 et seq.

الکترونیک این مهم را در کشورها انجام می‌دهند.[1] دفاتر خدمات صدور گواهی امضای الکترونیک پس از درخواست متقاضی و ثبت اسم، دو کلید در اختیار متقاضی قرار می‌دهند؛ به عبارت دیگر، یک کلید خصوصی در اختیار صاحب امضا قرار می‌گیرد و یک کلید عمومی که در فهرست مرجع گواهی قرار دارد. مرجع گواهی امضای الکترونیک تضمین می‌کند که کلید عمومی مندرج در فهرست به درستی ایجاد و اعلام شده است و ثبت اسم و هویت دارندهٔ کلید خصوصی که منطبق با کلید عمومی است، نزد مرجع گواهی وجود دارد.

در پایانِ این بحث لازم است تأکید گردد که فقدان امضای الکترونیک نمی‌تواند در امر انتساب داده پیام اختلال ایجاد کند؛ چرا که امضا تنها یکی از شیوه‌ها و ابزار سودمند انتساب محسوب می‌شود و نه همه شیوه‌ها؛ مثلاً پیام‌های حاصل از یک نمابر (فاکس) داده پیام تلقی می‌گردد؛[2] داده پیامی که فاقد امضا به آن مفهومی که امضا در دنیای الکترونیک دارد، است. محتویات داده پیام اعم از این که واجد امضا باشد یا خیر، ممکن است برای امر انتساب کافی باشد؛ چرا که از نظر ما عمل ارسال داده پیام چه از طریق ایمیل باشد و چه از طریق فاکس، خود به تنهایی می‌تواند امضا محسوب گردد.

۳.۲. اقدامات ثالث

بند (ب) مادهٔ ۱۹ قانون تجارت الکترونیک ایران با اقتباس از مادهٔ ۱۳ مقررات نمونه آنسیترال برای تجارت الکترونیک، فرض دیگری را مطرح کرده است که طی آن دریافت‌کننده می‌تواند فرض کند که داده پیام از ناحیه ارسال‌کننده فرستاده شده است؛ در صورتی که داده پیام ناشی از اعمال ثالثی باشد که به دلیل رابطه‌اش با اصل ساز به روش مورد استفادهٔ وی دسترسی داشته است.[3]

لازم به تأکید است که منظور از دسترسی در مقررات مورد بحث، دسترسی مجاز است؛ در غیراین صورت، مورد از شمول مفاد قانون خارج و اصولاً داده پیام قابل انتساب به ارسال‌کننده تلقی نخواهد شد. در روش مقرر در بند (ب) مادهٔ ۱۹، مخاطب از اعتماد به این واقعیت که ثالث

1. Loc. Cit; PP. 55 et Seq. See also Warwick Ford, *Computer Communications Security: Principles, Standard Protocols and Techniques*, Published by Prentice Hall, Englwood Cliffs, NJ, 1994, PP. 93-101.

ماده ۳۱ قانون تجارت الکترونیک ایران.

2. United Nations Commission on International Trade Law, Op. Cit., Note 103, P. 46; See also *UETA* Official Comments on Paragraph 3 of the Official Comments to Section 9.

3. United Nations Commission on International Trade Law, Op. Cit., Note 100, P. 44.

داده پیام را به دلیل ارتباطی که با ارسال‌کننده (اصل ساز) داشته، ارسال کرده است، داده پیام را منسوب به اصل ساز تلقی می‌کند. پرسشی که در اینجا مطرح می‌گردد، این است که ثالث چه شخصی می‌تواند باشد و ارتباط وی با ارسال‌کننده داده پیام به چه نحو است؟

مصداق بارز ثالث، قسمت دوم بند (الف) مادهٔ ۱۸ است. ثالث شخصی است که به روش اصل ساز به طور مجاز دسترسی دارد و ممکن است نماینده، وکیل، منشی و مدیران شرکت، کارشناسان، کارکنان اصل ساز یا اشخاص وابسته به او (و به طور کلی شامل هر شخصی که به موجب توافق قبلی با اصل ساز، پیامی از جانب وی ارسال می‌کنند) باشد. مثلاً وضعیتی را فرض کنیم که در آن دو شرکت مرتبط، یکی شرکت اصلی به نام «الف» و دیگری شرکت فرعی تحت کنترل به نام «ب» در امر تجارت مشغول به کارند. هر دو شرکت به ترتیب دارای دو وب‌سایت اصلی و فرعی با دو نام مختلف دامنه هستند. در وب‌سایت اصلی کالاهای مورد فروش، معرفی و در وب‌سایت فرعی قیمت کالاها اعلام می‌شود (ایجاب الکترونیک از سوی ب). گرچه ایجاب فروش از سوی «ب» پست شده است، مخاطب می‌تواند این ایجاب را ارسال شده از سوی «الف» تلقی نماید.

در دعوای Chwee Kin Keong & Others v. Digilandmall.com Pte Ltd [2005] SGCA 2[1]. خوانده، شرکت دیجی‌لند در وب‌سایت خود (شرکت D) و وب‌سایت دیگر، متعلق به شرکت هیولت پاکارد (شرکت HP) و نیز وب‌سایت سوم دیگر مرتبط با شرکت خوانده (شرکت DIL) در امر معرفی، قیمت‌گذاری و فروش چاپگر لیزری مشارکت می‌کند. از سوی شرکت DIL، قیمت چاپگر به اشتباه ۶۶ دلار اعلام و در سایت‌های یادشده پست و ثبت می‌گردد. تا زمان کشف این اشتباه، در مجموع ۱۶۰۶ چاپگر تا تاریخ ۱۴ ژانویه ۲۰۰۳ از سوی ۷۸۴ شخص سفارش داده می‌شود. پس از کشف خطای قیمت‌گذاری، شرکت دیجی‌لند به سرعت اطلاعات نادرست را اصلاح و قیمت واقعی (۳۸۵۴ دلار) را در وب‌سایت‌ها درج و از اجرای قراردادهای

1. A/CN.9/SER.C/ABSTRACTS/50 II; Decision date13/01/2005; United Nations, United Nations Commission on International Trade Law, Case Law on Uncitral Texts (CLOUT), A/CN.9/SER.C/ABSTRACTS/50 (Decision date13/01/2005), 26 August 2005, PP. 10-12. See also Case Note, Digital Evidence and Electronic Signature Law Review, at 114-15. Available at: file:///C:/Users/dear/Downloads/1763-Article%20Text-2391-1-10-20140120.pdf

همچنین برای دسترسی کامل به رأی، رک:

https://www.supremecourt.gov.sg/docs/default-source/module-document/judgement/2005-sgca-2.pdf

منعقده به دلیل اشتباه در قیمت ارسال‌شده خودداری می‌کند. خریداران به مادۀ ۱۳-۳ بند ب قانون معاملات الکترونیک سنگاپور استناد کرده و تقاضای الزام فروشنده به تحویل پرینترها را می‌نمایند. در مقابل، شرکت خوانده به استناد بند (ب) ماده ۱۳-۴ قانون معاملات الکترونیک سنگاپور، مدعی می‌گردد که به دلیل تفاوت فاحش قیمت اعلام‌شده و قیمت واقعی و کوتاه بودن مدت زمان اعلام قیمت، هر انسانی عاقلی درمی‌یابد که قیمت به اشتباه درج شده است و نمی‌تواند منتسب به اصل ساز باشد. استدلال خوانده مورد پذیرش دادگاه بدوی قرار می‌گیرد. دادگاه تجدید نظر نیز با پذیرش استدلال خوانده و با لحاظ آگاهی بعضی از خواهان‌ها از اشتباه در قیمت‌گذاری، در تأیید رأی دادگاه بدوی در حکم خود،،قانون معاملات الکترونیک سنگاپور را که مقتبس از مقررات آنسیترال برای تجارت الکترونیک است (بند ب ماده ۱۳-۴)، اعمال و خریدها را به دلیل اشتباه یک‌جانبه، باطل و ادعاهای خواهان‌ها را بر همین اساس رد کرد.

نتایج مهمی از رأی یادشده حاصل می‌شود. انتساب داده پیام از طرق زیر به اصل ساز منتسب گردید:

۱. روش معرفی (مخاطب از طریق سایت‌های D و DIL و نیز از طریق ثالث یعنی وب‌سایت HP به قیمت پرینتر دسترسی پیدا می‌کند و آن را ارسال‌شده از سوی خوانده تلقی می‌کند).

۲. اقدامات شخص ثالث (مخاطب از طریق ثالث یعنی وب‌سایت HP به قیمت پرینتر دسترسی پیدا می‌کند و آن را ارسال‌شده از سوی خوانده تلقی می‌کند).

نتیجه‌گیری

با توضیح این مطلب که مقنن مقررات انتساب داده پیام را در دو قالب ثبوتی و اثباتی بیان داشته است، سعی کردیم مفهوم دقیق انتساب داده پیام را تشریح کنیم. نتیجهٔ حاصل از آن احراز سه عنصر به این شرح است:

- آفرینش داده پیام یا ارسال داده پیام؛
- تأیید هویت دارندهٔ منبع آفرینش داده پیام و یا ارسال داده پیام؛
- احراز هویت خالق یا ارسال‌کنندهٔ داده پیام برای انتساب داده پیام.

در ادامهٔ بحث، احکام جنبه‌های ثبوتی انتساب داده پیام را تفسیر و بحث مهم جنبه‌های حقوقی اثبات انتساب داده پیام را در سه فرض، یعنی روش معرفی و توافقی و اقدامات شخص ثالث را مطرح و تفسیر کردیم و مباحث مهم فنی اثبات انتساب داده پیام چون روش‌های عادی، مطمئن و رویه ایمن را مطرح کردیم و دیدیم که روش مطمئن نه به معنای رویهٔ ایمن، بلکه به نوعی یکی از مصادیق استفاده از رویهٔ ایمن است؛ به عبارت دیگر، می‌توان چنین گفت که بین رویهٔ ایمن و روش مطمئن رابطهٔ عموم و خصوص مطلق جاری است؛ یعنی روش مطمئن یک رویهٔ ایمن است، اما هر رویهٔ ایمنی ممکن است روش مطمئن محسوب نگردد. رویهٔ ایمن از لحاظ فنی، روشی است برای احراز هویت یک شخص یا تأیید صحت یک داده پیام. این واژه متضمن رویه‌ای است که مستلزم استفاده از الگوریتم‌ها یا سایر کدها، کلمات یا ارقام شناسایی، رمزنگاری یا تصدیق با پاسخ برگشت و سایر طرق تصدیق است و دیدیم که این رویه می‌تواند بسیار ساده باشد؛ مانند تماس از طریق کانال ارتباطی دیگر مثل خط تلفن به منظور تأیید و احراز هویت ارسال‌کنندهٔ داده پیام یا استفاده از نام مادر یا شخص دیگر و یا از طریق شماره شناسایی شخصی. از سوی دیگر، دیدیم که رویهٔ ایمن ممکن است خیلی پیچیده باشد؛ مانند استفاده از عملیات رمزنگاری (استفاده از کلید خصوصی و کلید عمومی) و امضای الکترونیک مطمئن.

در نهایت، مفهوم شخص ثالث و مصادیق آن را که به نحو بسیار مبهم در قانون آمده است، روشن کردیم. در روش مقرر در بند (ب) مادهٔ ۱۹، مخاطب از اعتماد به این واقعیت که ثالث داده پیام را به دلیل ارتباطی که با ارسال‌کننده (اصل ساز) داشته، ارسال کرده است، داده پیام را منسوب به اصل ساز تلقی می‌کند. دیدیم ثالث شخصی است که به روش اصل ساز به طور مجاز

دسترسی دارد و ممکن است نماینده، وکیل، منشی و مدیران شرکت، کارشناسان، کارکنان اصل ساز یا اشخاص وابسته به او و به طور کلی شامل هر شخصی که به موجب توافق قبلی با اصل ساز، پیامی از جانب وی ارسال می‌کنند، باشد.

در آخر پیشنهاد می‌گردد:

- مادۀ ۱۹ به شرح پیشنهادات مندرج در این مقاله اصلاح شود.
- موضوعات مهم از جمله روش‌های انتساب، خصوصاً استفاده از رویۀ ایمن به صورت جامع و واضح در اصلاحات بعدی قانون مد نظر قرار گیرند.

فهرست منابع

الف) منابع فارسی

کتاب

۱. دهخدا، علی اکبر، ***لغت نامه اینترنتی دهخدا***.

۲. جعفری لنگرودی، محمد جعفر، ***دانش نامه حقـوقی***، موسسـه انتشـارات امیرکبیـر، چـاپ پنجم، ۱۳۷۵.

۳. جعفری لنگرودی، محمدجعفر، ***دوره پنج جلدی مبسوط در ترمینولوژی حقوق***، جلد ۱، گنج دانش.

۴. معین، محمد، ***فرهنگ آنلاین معین***.

ب) منابع انگلیسی

Books

5. Lance, Rose, *Netlaw: Your Rights in the Online World*, Osborne Mc Graw-Hill, 1995.
6. National Conference of Commissioners on Uniform State Laws, *Uniform Electronic Transactions Act* (1999), (*UETA*), Drafted by the National Conference of Commissioners on Uniform State Laws (with Prefatory Note and Comments), 1999.
7. Savin, Andrej, *EU Internet Law*, Elgar European law, Edward Elgar Pub., 2013.
8. Schellekens, M. H. M., *Electronic Signatures: Authentication Technology from a Legal Perspective*,TMC Asser Press, The Hague The Netherlands, 2004.
9. United Nations, United Nations Commission on International Trade Law, *Promoting Confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods*, United Nations, Vienna, 2009.
10. United Nations, *United Nations Uncitral Model Law on Electronic Commerce, Guide to Enactment 1996 with additional article 5 as adopted in 1998*, United Nations, New York, 2002.

11. United Nations, *Uncitral Model Law on Electronic Signature with Guide to Enactment 2001*, United Nations, New York, 2002.
12. Warwick Ford, *Computer Communications Security: Principles, Standard Protocols and Techniques,*Prentice Hall, Englwood Cliffs, NJ, 1994.
13. Yun, Zhao, *Dispute Resolution in Electronic Commerce*, Martinus Nijhoff Publishers, 2005.

Articles

14. Agris, Repss and Ilze Znotina, "Electronic Evidence in Latvia", *Digital Evidence and Electronic Signature Law Review*, Volume 8, 2100.
15. Anjanette, H., Raymond & J Benjamin Lambert,"Technology, E-commerce and the Emerging Harmonization: The Growing Body of International InstrumentsFacilitating Ecommerce and the Continuing Need to Encourage Wide Adoption", *International Trade andBusiness Law Review*, Volume 17, 2014.
16. Boss, Amelia, H., "Searching for Security in the Law of Electronic Commerce", *Nova Law Review*, Volume 23, Issue 2, 1999.
17.Froomkin, A., Michael, "The Essential Role of Trusted Third Parties in Electronic Commerce", *Oregon Law Review*, Vol. 75, 1996.
18. Mikellyn, Jason, Johnson, Charles, Transactions of the Centre for Business Law, *Consequences of and Problems with Electronic Contracts*, University of the Free State, Chapter 8, Issue 37, 2005.
19. Mann, Ronald J., Warren, Elizabeth: Westbrook, Jay Lawrence,_ *Comprehensive Commercial Law 2018: Statutory Supplement (Supplements) Paperback*, 2018, Wolters Kluwer.
20. Manuel, Alba, "Order out of Chaos: Technology, Intermediation, Trust, and Reliability as the Basis for the Recognition of Legal Effects in Electronic transactions", *Creighton Law Review*, Volume 47, 2014.
21. Phang, A., & Seng, D., "The Singapore Electronic Transactions Act 1998 and the Proposed Article 2B of the Uniform Commercial Code",*International Journal of Law and Information Technology*, Volume 7, 1999.
22. Pistorius, Tana, "Nobody Knows You're a Dog: The Attribution of Data Messages", *South African Mercantile Law Journal*, 2002, Volume 14.
23. Tan, Bryan (Singapore correspondent), "Case Note", *Digital Evidence and Electronic Signature Law Review*, 2005, at 114-15. Available at:

file:///C:/Users/dear/Downloads/1763-Article%20Text-2391-1-10-20140120.pdf

24. Yaman Akdeniz& Others, "Cryptography and Liberty: 'Can the Trusted Third Parties Be Trusted? A Critique of the Recent UK Proposals", *Journal of Information Technology*, Vol. 2, 1997.

Cases

25. *Central Illinois Light Company (CILCO) v. Consolidation Coal Company (Consol)*, United States District Court for the Central District of Illinois, 30 December 2002, Federal Supplement, 2nd series, vol. 235, p. 916.
26. *Chwee Kin Keong & Others v. Digilandmall.com Pte Ltd* [2005] SGCA 2 (A/CN.9/SER.C/ABSTRACTS/50 II; Decision date13/01/2005; United Nations, United Nations Commission on International Trade Law, Case Law on UNCITRAL Texts (CLOUT)).
27. *Commonwealth Aluminum Corporation v. Stanley Metal Associates*, United States District Court for the Western District of Kentucky, 9 August 2001, Federal Supplement, 2nd series, vol. 186, p. 770.
28. *Dickens v. State*, 927 A.2d 32, 36-37 (Md. Ct. Spec. App. 2007).
29. *Lorraine v. Markel Am. Ins. Co*., 241 F.R.D. 534, 554 (D. Md. 2007).
30. *People v. Brown*, A122791, 2009 WL 1878704, at *3 (Cal. Ct. App. June 30, 2009).
31. *Sea-Land Service, Inc. v. Lozen International, LLC*, United States Court of Appeals for the Ninth Circuit, 3 April 2002, Federal Reporter, 3rd series, vol. 285, p. 808.
32. *State v. Taylor*, 632 S.E.2d 218, 230 (N.C. Ct. App. 2006).
33. *Superhighway Consulting, Inc. v. Techwave, Inc*., United States District Court for the Northern District of Illinois, Eastern Division, 16 November 1999, U.S. Dist. LEXIS 17910.
34. *Talada v. City of Martinez*, 656 F. Supp. 2d 1147, 1158 (N.D. Cal. 2009).
35. *United States v. Safavian*, 435 F. Supp. 2d 36, 40 (D.D.C. 2006).

Acts

36. Singapore's Electronic Transaction Act Revised 2011.
37. Australian Electronic Transactions Act 1999.
38. Uniform Electronic Transactions Act (UETA), Drafted by the USA National Conference of Commissioners on Uniform State Laws,(1999).