Shiraz University
RICeST
ISC
ISSN: 2008-7926

Journal of
Legal Studies
Scientific

Vol. 18, Issue 2, Suumer 2026

JLS

Journal of Legal Studies
Journal Homepage: https://jls.shirazu.ac.ir/
doi: https://10.22099/jls.2025.53069.5314

Research Article

Computer-related Forgery in the Iranian Legal System with Emphasis on the Condition of Data Admissibility

Reza Hadizadeh*

PhD in Criminal Law and Criminology, Faculty of Law and Political Science, University of Mazandaran; Babolsar, Iran

Article history: Received: 27-04-2025 Accepted: 05-08-2025

Abstract

Introduction

Computer-related forgery is a modern crime and a challenging topic in criminal law. The conditions for establishing this offense, particularly the requirement of "admissibility" as mentioned by the legislator in Clause “A” of Article 734 of the Islamic Penal Code, are ambiguous. Legal scholars have proposed various interpretations of what constitutes "admissible" data. These include data with evidentiary value, legal significance, judicial weight, or admissibility in legal proceedings—whether in defense or claim. Still, some of the provided definitions are unclear and need further explanation, which can lead to different interpretations when applying them to real-world cases. This research aims to examine the concept and conditions for establishing computer-related forgery and to clarify the boundaries between this offense and other similar cases involving data creation or alteration.

Please cite this article as:
Hadizadeh, R (2026). Computer-related Forgery in the Iranian Legal System with Emphasis on the Condition of Data Admissibility. *Journal of Legal Studies*, *18*(2), 225-266.
doi: https://10.22099/jls.2025.53069.5314.

* Corresponding author:
E-mail address: hadizadehr@yahoo.com

Method

An analytical-descriptive approach was employed in this research. By reviewing related legislation including the Islamic Penal Code, the Code of Criminal Procedure, the Electronic Commerce Act, and the "Regulations on Collection and Admissibility of Electronic Evidence" enacted in 2014, legal concepts such as admissibility, undeniability, validity, and data integrity were analyzed. Additionally, scholars' opinions and practical examples were examined to enhance the understanding of computer-related forgery.

Findings

Article 685 of the Code of Criminal Procedure refers to three concepts related to data admissibility: "undeniability", "validity," and "integrity." Considering these terms, which are also used in various parts of the Regulations on Electronic Evidence Collection and Admissibility(enacted 2014), and by taking into account the Electronic Commerce Act, the conditions for admissible data can be linked to the concept of "secure data messages" under the Electronic Commerce Act. According to Article 14 of the Electronic Commerce Act, data messages created and maintained securely are considered valid documents and "admissible" in judicial and legal authorities. Article 15 states that reliable data messages, electronic records, and electronic signatures are undeniable; one can only claim that the "message data" is forged or prove that the "message data" has been legally invalidated in some way. In other words, firstly, reliable message data is admissible according to the stipulation of Article 14 of the Electronic Commerce Law, and secondly, since reliable message data is undeniable according to Article 15 of the Electronic Commerce Law, and one of the characteristics of admissible data is that it is undeniable, it can be seen that admissible data is the same as reliable message data.

If we reject the idea that admissible data must meet the criteria of a secure data message, then implementation of security protocols within the software or system where the forgery occurs becomes crucial. In this context, it is essential that the creation or alteration of the data can be reasonably attributed to someone other than the actual perpetrator. Legal value, the potential to mislead ordinary individuals, and actual or potential harm are additional conditions of computer-related forgery, deriving from the notions of admissibility, forgery concepts, traditional forgery conditions, and legal principles. The perpetrator's intent to present the forged data to others or authorities as original, is essential for establishing the crime.

Conclusion

To reduce existing ambiguities, it is necessary to revise the law and clearly

define the conditions for establishing the crime of computer-related forgery. In any case, Admissible data can be regarded as equivalent to reliable data messages, or at least the implementation of security measures—such as proper authentication—should be regarded as a requirement of computer-related forgery. According to the mentioned conditions, actions like creating a receipt using receipt-generating software, producing and altering an image of a certificate, merely creating a social media account under someone else's name and details, and sending messages without meaningful or legal content from another person's SIM card cannot be classified as computer-related forgery. In contrast, cases such as intruding into secure banking systems and creating payment slips in the system's records, sending a message with a SIM card belonging to someone else that has legal value can be subject to the crime of computer-related forgery.

Keywords: Computer-Related Forgery, Admissible, Cyberspace, Data Integrity, Data Non-repudiation.

.

مجله مطالعات حقوقی علمی
شاپا: ۷۹۲۶-۲۰۰۸

دوره هجدهم، شماره دوم، تابستان ۱۴۰۵

مجله مطالعات حقوقی
Journal Homepage: https://jls.shirazu.ac.ir/
doi: https://10.22099/jls.2025.53069.5314

JLS

مقاله پژوهشی

جعل رایانه‌ای در نظام حقوقی ایران با تأکید بر شرط قابلیت استناد داده

رضا هادی‌زاده *

دانش‌آموخته دکتری، حقوق کیفری و جرم‌شناسی، دانشکده حقوق و علوم سیاسی، دانشگاه مازندران؛ بابلسر، ایران

اطلاعات مقاله | تاریخ دریافت: ۱۴۰۴/۰۲/۰۷ | تاریخ پذیرش: ۱۴۰۴/۰۵/۱۴

چکیده

بند «الف» از ماده ۷۳۴ قانون مجازات اسلامی در خصوص جعل رایانه‌ای به «تغییر یا ایجاد داده‌های قابل استناد یا ایجاد یا واردکردن متقلبانه داده به آن‌ها» اشاره دارد. بااین‌حال، مقصود از شرط «قابل استناد» به‌عنوان شرط بنیادین ذکرشده در قانون، مشخص نیست و داشتن ارزش اثباتی، قابل استناد بودن در مقام دفاع و دعوا و داشتن ارزش قضایی ازجمله تعاریف ذکر شده توسط حقوق‌دانان در مورد عبارت مذکور است. با استفاده از ماده ۶۸۵ قانون آیین دادرسی کیفری و دیگر مواد قانونی می‌توان گفت عدم خدشه به اوصاف «صحت و تمامیت، اعتبار و انکارناپذیری داده‌ها» در تحقق قابل استناد بودن داده شرط است؛ همچنین می‌توان با استفاده از قانون تجارت الکترونیک، داده قابل استناد را داده‌ای دانست که با شرایط داده پیام مطمئن منطبق است؛ به عبارتی هر داده پیام دارای ارزش اثباتی، لزوماً داده قابل استناد نیست. درهرحال، تردیدی نیست داده‌هایی که در مورد آن‌ها تمهیدات امنیتی به کار برده نشده است و با لحاظ مواردی مانند عدم انتساب معقول، آسیب‌پذیری در برابر سوءاستفاده و دست‌کاری، قابل‌اطمینان نباشند، موضوع جعل رایانه‌ای نخواهند بود که برای نمونه می‌توان

استناد به این مقاله:
هادی‌زاده، رضا (۱۴۰۵). جعل رایانه‌ای در نظام حقوقی ایران با تأکید بر شرط قابلیت استناد داده. *مجله مطالعات حقوقی*. ۱۸. (۲). ۲۶۶-۲۲۵.

* نویسنده مسئول: E-mail address: hadizadehr@yahoo.com

به ایجاد صفحه در شبکه‌های اجتماعی به نام دیگری در حالتی که احراز هویت مناسب انجام صورت نگرفته است اشاره کرد. به‌علاوه، قابلیت انتساب معقول داده، داشتن ارزش حقوقی و امکان به اشتباه انداختن اشخاص متعارف از دیگر شرایط جعل رایانه‌ای است که این شرایط از عبارت قابل استناد، مفهوم جعل، شرایط جعل سنتی و اصول حقوقی قابل‌فهم است.

واژگان کلیدی: جعل رایانه‌ای، قابل استناد، فضای مجازی، تمامیت داده، انکارناپذیری داده.

سرآغاز

به دلیل ظرفیت‌های فضای سایبری، تقریباً تمامی جنبه‌های زندگی مردم دنیا به این فضا وابسته شده است و با توجه به تهدیداتی که از طرف فناوری‌های سایبری وجود دارد، امنیت در فضای سایبری به دغدغه اصلی جامعه بین‌المللی تبدیل شده است (Farshasaeed et al, 2021: 2). یکی از موارد حائز اهمیت که تهدید در فضای مجازی است شبیه‌سازی و جعل رایانه‌ای است.

موضوع نوشتار حاضر با عناوینی نظیر جعل در بستر فناوری‌های اطلاعات و ارتباطات (Ghanad, 2011)، «جعل دیجیتال» که اعم از جعل الکترونیکی و سرقت هویت دانسته شده است (Sadiku et al, 2017: 26) در برخی از آثار عربی با عنوان «جعل الکترونیکی»[1] (Al-Ardi, 2012) و در کنوانسیون بوداپست با عنوان «جعل مرتبط با رایانه»[2] موردبحث واقع شده است؛ در حقوق ایران نیز به موجب ماده ۶۸ قانون تجارت الکترونیک مصوب ۱۳۸۲ با عبارت «جعل کامپیوتری» و در قانون جرائم رایانه‌ای با عبارت «جعل رایانه‌ای» جرم‌انگاری و برای آن مجازات تعیین شده است.

بااین‌حال، وضعیت حقوقی موارد بسیاری از حیث انطباق یا عدم انطباق با بزه، جعل رایانه‌ای نامشخص است که ابهاماتی را از جهت نظری قابل‌طرح ساخته است؛ ازجمله آنکه ممکن است شخصی تصویر جعلی از گواهی اشتغال به تحصیل، کارت پایان خدمت یا مدرک تحصیلی صرفاً به شکل داده تهیه و برای مرجعی ارسال کند یا اینکه با استفاده از نرم‌افزار رسید ساز، سند پرداخت جعلی یا هرگونه سند دیگری که نشان از پرداخت وجه دارد ایجاد کند یا در نرم‌افزار یا پایگاه‌های مرتبط با شبکه‌های اجتماعی یا ارتباطی، حساب کاربری با نام و مشخصات دیگری ایجاد و مبادرت به

---

۱. التزویر الإلکترونی.

2 . Computer-related forgery.

ارسال پیام به اشخاص از طریق آن کند؛ در این موارد مشخص نیست آیا مرتکب با عنوان جعل رایانه‌ای قابل‌تعقیب است یا خیر؟

ابهام فوق ناشی از عدم تعریف قانون‌گذار از جعل رایانه‌ای و عدم تبیین شرایط و اوصاف تحقق بزه است؛ چه ماده ۷۳۴ ق.م.ا تنها به اینکه داده باید «قابل استناد» باشد، اشاره دارد که عبارت مذکور مبهم و مفهوم آن روشن نیست و استنباط‌های مختلف در مورد آن قابل‌طرح است. ابهامی که هرچند توسط مجمع مشورتی حقوقی شورای نگهبان به تاریخ ۱۳۸۷/۱۲/۱۳ مطرح شد[1]، اما در ایرادات شورای نگهبان لحاظ نشد و درنتیجه، ماده مذکور بدون تغییر و رفع ابهام در مصوبه نهایی مجلس باقی ماند.

نگارنده اذعان دارد، به دلیل کلی‌گویی و ابهام قانون از یک‌سو و جدید بودن برخی از مفاهیم مرتبط با جرائم رایانه‌ای از سوی دیگر، تبیین چارچوب دقیق و بیان قاعده‌ای که با آن به سهولت بتوان تمام مصادیق را بر جرم موردبحث منطبق کرد دشوار است. بااین‌حال، نوشتار حاضر می‌کوشد با تفکیک مباحث به دو گفتار شرایط جعل رایانه‌ای را به شرح ذیل تبیین کند.

۱. داده قابل استناد در قانون

در این مبحث، به اوصاف ذکر شده توسط قانون‌گذار برای داده قابل استناد، مفهوم آن‌ها و ضرورت آن‌ها برای قابل استناد بودن داده و اینکه آیا اساساً شرط قابل استناد بودن در جعل داده لازم است موردبحث واقع می‌شود.

---

۱ . در نظریه این مجمع آمده است: اولاً «داده‌های قابل استناد» از حیث تعریف، مواجه با ابهام است. ثانیاً مشخص نیست مقصود از «قابلیت استناد داشتن داده‌ها» نزد چه شخص یا مقامی موردنظر است؟

۱-۱. بررسی اشتراط قابل استناد بودن داده

بند الف ماده ۷۳۴ ق.م.ا در خصوص جعل رایانه‌ای متشکل از دو قسمت است که عبارت‌اند از ۱. تغییر یا ایجاد داده‌های قابل استناد ۲. ایجاد یا واردکردن متقلبانه داده به آن‌ها. در ماده مذکور به «تغییر»، «ایجاد» و «واردکردن» به‌عنوان رفتار فیزیکی جرم موردبحث اشاره کرده است. برخی (Mohammadi Ferdouei, 2018: 468) در بیان تفاوت بین وارد کردن و ایجاد کردن داده‌ها معتقدند که منظور از ایجاد کردن داده به وجود آوردن یک داده جدید است که هیچ‌یک از اجزا آن از قبل وجود نداشته است ولی در وارد کردن داده، اجزا آن از قبل وجود داشته است. درهرحال فقدان دقت کافی در تدوین ماده ۷۳۴ ق.م.ا آشکار است؛ اولاً این پرسش قابل‌طرح است که در ماده مذکور مرجع ضمیر «آن‌ها» در انتهای بند مذکور چیست. چنانچه پاسخ این باشد که مرجع ضمیر «آن‌ها» عبارت «داده‌های قابل استناد» است با پرسش دیگری مواجه می‌شویم که ذکر واژه «ایجاد» داده در انتهای بند «الف» به چه سبب بوده است زیرا در ابتدای بند مذکور نیز به واژه مذکور اشاره شده است؛ همچنین دلیل ذکر عبارت «وارد کردن» داده به داده دیگر در انتهای بند «الف» به جهت اینکه در ابتدای بند مذکور از واژه «تغییر» استفاده شده است و وارد کردن داده به داده دیگر از مصادیق تغییر است مشخص نخواهد بود. از طرف دیگر، صرف‌نظر از اینکه واژه «ایجاد» و عبارت «وارد کردن» در معنای عام، اعم از یکدیگر است و ذکر ایجاد متقلبانه داده در داده قابل استناد یا عبارت وارد کردن داده به داده قابل استناد کافی بود، اساساً نیازی به قسمت دوم بند مذکور یعنی عبارت «یا ایجاد یا واردکردن متقلبانه داده به آن‌ها» نیست؛ زیرا با ذکر عبارت «تغییر» داده قابل استناد نیازی به ذکر موارد مذکور در قسمت دوم بند مذکور از این جهت که این موارد از مصادیق تغییر هستند نبوده است.

دوم آنکه، در قسمت دوم بند ماده ۷۳۴ ق.م.ا به واژه متقلبانه اشاره شده است که اولاً، مقصود از واژه مذکور چندان واضح نیست و ضروری بود در قسمت نخست بند مذکور نیز به واژه متقلبانه اشاره می‌شد. این امر موجب شده است برخی (Gerayeli,

2010: 171) معتقد باشند وصف متقلبانه صرفاً ناظر به قسمت دوم بند مذکور است و بین دو قسمت ماده مذکور تفاوت وجود دارد. به همین شکل، در نظریه کارشناسی درباره لایحه جرائم رایانه‌ای با شماره مسلسل ۷۵۵۲ (2005: 11) در خصوص تغییرات حاصله در مورد ماده مرتبط با جعل آمده است «... [در این بند] دو قسم رفتار فیزیکی مدنظر قرار گرفته ... یکی حذف یا تغییر یا متوقف کردن داده‌های قابل استناد که در اینجا داده‌ها باید نزد مراجع قانونی قابلیت استناد داشته باشند و دیگری ایجاد یا وارد کردن داده‌ها که چون این داده‌ها برخلاف حالت قبلی با قصد تقلب وارد می‌شوند لازم نیست قابل استناد باشند و شامل هر نوع داده‌ای هستند».

صحت این برداشت محل تردید جدی است؛ نخست آنکه مرجع ضمیر «آن‌ها» در انتهای ماده، داده قابل استناد است. دوم آنکه واژه متقلبانه ناظر به هر دو قسم بند الف ماده ۷۳۴ ق.م.ا است؛ زیرا تفاوت ماهوی بین دو شق نخست و دوم از بند الف ماده مذکور وجود ندارد که تفاوت حکم دو حالت را منطقی سازد. از طرفی، ذکر واژه متقلبانه حاکی از عنصر روانی مرتکب و انگیزه وی در ایجاد و تغییر داده است که قانون‌گذار برای تحقق جرم لازم دانسته است؛ از یک منظر، عنصر روانی به چهار جزء ۱. سوءنیت عام ۲. سوءنیت خاص ۳. علم به موضوع ۴. انگیزه قابل‌تقسیم است. سوءنیت عام قصد رفتار و در جرم جعل رایانه‌ای قصد ایجاد یا تغییر داده است؛ از طرفی انگیزه دلیل ارتکاب جرم و به بیان دیگر پاسخ مرتکب به چرایی ارتکاب جرم است. از این جهت، انگیزه افراد در ارتکاب جرائم می‌تواند متفاوت باشد و برای مثال ارتکاب قتل برای سرقت، انتقام، از بین بردن دلیل ارتکاب جرم و ... باشد. انگیزه صرفاً در جرائمی که قانون‌گذار وجود انگیزه خاص را لازم بداند جزء عناصر رکن روانی است و در غیر این صورت می‌تواند صرفاً در مجازات مؤثر باشد. درواقع واژه «متقلبانه» حاکی از انگیزه مرتکب است و به عبارتی شخص ایجاد یا تغییر داده را باید با قصد تقلب انجام داده باشد؛ قصد تقلب یعنی قصد ارائه آن به شخص یا مراجعی برای اینکه آن را به‌عنوان اصل در نظر گرفته و درنتیجه از ارائه آن به‌طور بالفعل یا بالقوه منتفع

شود. در تقویت این استنباط می‌توان به متن اولیه ماده اشاره کرد؛ متن اولیه ماده بدین شرح که «هر کس با قصد تقلب داده‌های رایانه‌ای قابل استناد تغییر داده یا ایجاد یا حذف یا متوقف کند جاعل محسوب» می‌شود رساتر مقصود مقنن را بیان کرده بود. به‌علاوه، قابل استناد بودن، به شرحی که خواهد آمد، شرط تحقق جرم جعل سنتی نیز است. همچنین در جعل سنتی ماده ۵۲۳ ق.م.ا با عبارت «به قصد تقلب» و در ماده ۶۸ قانون تجارت الکترونیک با عبارت «تا با ارائه آن به مراجع اداری،قضایی، مالی و غیره به‌عنوان «داده پیام»های معتبر است به قصد تقلب و به عبارتی عنصر روانی جرم اشاره دارند که مواد مذکور نیز مؤید این استنباط است که واژه متقلبانه عنصر روانی جرم و به‌نوعی انگیزه ارتکاب جرم است که قانون‌گذار برای تحقق جرم شرط کرده است. همچنین در ماده ۱۰ «کنوانسیون عربی برای مبارزه با جرائم فناوری اطلاعات» به جعل با هدف استفاده از آن به‌عنوان مدرک معتبر[1] و در ماده ۶ کنوانسیون بوداپست نیز به هدف مرتکب دایر بر در نظر گرفتن یا اقدام بر اساس داده‌ها غیر معتبر به‌عنوان داده‌های معتبر اشاره شده است. ماده ۱۸۶ قانون مجازات عراق نیز به قصد فریب[2] اشاره شده دارد و قصد مرتکب باید استفاده از سند مجعول به‌عنوان سند معتبر باشد (Al-Ardi, 2012: 160).

۱-۲. دیدگاه حقوق‌دانان در مورد تعریف داده قابل استناد

در جرائم موضوع مواد ۷، ۹، ۱۰، ۱۳، ۱۶، ۱۸ و ۲۵ قانون جرائم رایانه‌ای نیز اصولاً رفتارهای فیزیکی جرم جعل داده یعنی تغییر یا ایجاد داده به نحوی وجود دارد؛ ضابطه‌ای که بتوان بر اساس آن جرائم موضوع مواد فوق را از جرم جعل رایانه‌ای تفکیک کرد، قید محوری ذکر شده توسط مقنن در بحث جعل داده یعنی عبارت «قابل

---

۱. بنیهٔ استعمالها کبینات صحیحهٔ.

۲. بقصد الغش

استناد» است؛ بااین‌حال، به جهت مبهم و کلی بودن عبارت مذکور و اینکه مقنن عبارت مذکور را تعریف نکرده است، تاب بیان نظرات متفاوت در تفسیر آن وجود دارد. در این راستا، دلیل بودن و داشتن ارزش اثباتی و اینکه در مراجع مختلف اداری، قضایی و غیره به‌عنوان داده پیام معتبر استعمال شود و در اثبات حق تضییع و انکار شده مؤثر باشد (Torki, 2010: 33) واجد ارزش حقوقی بودن (Azizi, 2019: 105) داده‌ای که در مقام دفاع یا دعوی قابل استناد باشد، نظیر امضای دیجیتال (Alipour, 2021: 210–211) و داده‌ای که در مقام دعوی یا دفاع قابل استناد بوده، به‌نحوی‌که به ظاهر به صحت و تمامیت، اعتبار و انکارناپذیری آن خدشه وارد نشود (Babaei, 2022: 22) واجد اعتبار بودن در محضر دادگاه و ایفای نقش در صدور رأی مقتضی (Moazenzadegan et al., 2015: 74; Moazenzadegan & Shayegan, 2009: 86)، داشتن ارزش اثباتی و اینکه در محاکم به‌عنوان سند قابل پذیرش باشند (Mohammad Nasl, 2013: 72)، مؤثر در اثبات و نفی امر و به تعبیر دیگر، داشتن ارزش قضایی (Amirian Farsani & Hosseini, 2019: 65) ازجمله معانی ذکر شده برای عبارت مذکور است. در خصوص تفاوت قابلیت استناد و عدم قابلیت استناد یک عنصر نظام حقوقی (صرف‌نظر از داده) نسبت به اینکه این عنصر اثر غیرمستقیم حقوقی در برابر اشخاص ثالث دارد یا خیر، اشاره شده است؛ به عبارتی، اشخاص ثالث این حق را دارند که عنصر حقوقی غیر قابل استناد را نادیده انگارند؛ ولی عنصر حقوقی قابل استناد نسبت به اشخاص ثالث نیز اعتبار دارد (Robati, Mohseni & Ghabouli Dorafshan, 2018: 118).

درهرحال، حتی با پذیرش هر یک از این معانی مذکور نیز مشکل مرتفع نشده و بررسی تطبیق مصادیق مشتبه بر آن‌ها می‌تواند محل بحث و ابهام باشد؛ مضافاً اینکه برخی از تعاریف مذکور خود مبهم بوده و نیازمند توضیح و تشریح است. قبل از بررسی مفهوم قابل استناد، لازم به ذکر است داشتن ارزش اثباتی که در برخی از تعاریف فوق بدان اشاره شده است در ماده ۶۸ قانون تجارت الکترونیک در باب جعل

کامپیوتری نیز شرط تحقق جرم مذکور دانسته شده است. ارزش اثباتی با مفهوم دلیل مرتبط است و اساساً سالموند (1907: 446) بیش از یک قرن پیش دلیل را «...هر واقعیت که دارای نیروی اثباتی است» تعریف می‌کند.

۳-۱. اوصاف قانونی داده قابل استناد

در این مبحث، سه مفهوم «انکارناپذیری»، «اعتبار»، «صحت و تمامیت» مورد بررسی قرار می‌گیرد؛ به این مفاهیم در ماده ۶۸۵ قانون آیین دادرسی کیفری اشاره شده است. همچنین در مواد مختلف آیین‌نامه «جمع‌آوری و استناد پذیری ادله الکترونیکی» مصوب ۱۳۹۳ از واژه‌های مذکور استفاده شده است؛ ازجمله بند «هـ» ماده یک و ماده ۷ به صحت و تمامیت، اعتبار و انکارناپذیری و مواد ۱۶، ۱۸ و ۳۵ به واژه‌های صحت، تمامیت و انکارناپذیری اشاره دارند.

۱-۳-۱. نکارناپذیری

یکی از اوصاف قابل‌ذکر برای عبارت «قابل استناد» در ماده ۷۳۴ ق.م.ا غیرقابل‌انکار بودن است که از این جهت، با سند از نوع رسمی آن مشابهت دارد؛ بدین توضیح که ماده ۱۴ قانون تجارت الکترونیک داده پیام‌های ایجاد و نگهداری شده به طریق مطمئن را در حکم سند معتبر و ***«قابل استناد»*** در مراجع قضایی و حقوقی دانسته است. از طرفی، طبق ماده ۱۵ قانون تجارت الکترونیک نسبت به «داده پیام» مطمئن[1]، سوابق الکترونیکی مطمئن و امضای الکترونیکی مطمئن انکار و تردید مسموع دانسته نشده است و مقرر شده است که تنها می‌توان ادعای جعلیت به «داده پیام» مزبور وارد کرد و یا ثابت کرد که «داده پیام» مزبور به جهتی از جهات قانونی از اعتبار افتاده است. این

۱. شرایط و مفهوم داده پیام مطمئن از مواد مختلف قانون تجارت الکترونیک ازجمله ماده ۲ و مبحث سوم قانون مذکور قابل استنباط است.

همان قاعده‌ای است که در مورد اسناد رسمی به موجب ماده ۱۲۹۲ قانون مدنی پیش‌بینی شده است[۱]؛ به عبارتی، قابل استناد بودن مرتبط با مطمئن بودن داده ایجاد شده است و از آثار مطمئن بودن داده ایجاد شده این است که قابل‌انکار و تردید نیست و این همان اثری است که به موجب قانون، بر اسناد رسمی و نه عادی مترتب است.

ممکن است در خصوص ماده ۱۴ قانون تجارت الکترونیک گفته شود؛ قانون‌گذار در مقام بیان تعریف داده قابل استناد نبوده است و از طرفی اثبات شی نفی ماعدا نمی‌کند؛ به عبارتی داده‌های ایجاد و نگهداری شده به نحو مطمئن واجد وصف قابل استناد هستند اما این بدان معنا نیست که سایر داده‌ها قابل استناد نیستند. از طرف دیگر، ماده ۱۴ قانون تجارت الکترونیک به این مطلب اشاره دارد که داده در حکم سند معتبر و قابل استناد است و مقصود قانون‌گذار، سند فیزیکی است[۲].

آنچه اشکال فوق را تقویت می‌کند آن است که هرچند بین امضای الکترونیک و امضای الکترونیک مطمئن و بین داده پیام با داده پیام مطمئن، تفاوت وجود دارد؛ اما امضای الکترونیک و داده پیام، ولو اینکه موصوف به وصف مطمئن نباشند ارزش اثباتی دارند؛ به عبارتی سند الکترونیک با محتوای داده پیامی فاقد شرایط اطمینان نیز دارای اعتبار است (Rouhbakhsh et al., 2022: 133–134)؛ زیرا اساساً داده پیام مستند به ماده ۶ قانون تجارت الکترونیک در مواردی که وجود یک نوشته ازنظر قانون لازم باشد مگر در موارد خاص، در حکم نوشته است و به موجب ماده ۷ قانون مذکور هرگاه قانون، وجود امضا را لازم بداند امضای الکترونیکی کافی است و مقصود از امضای الکترونیکی در ماده مذکور اعم امضای الکترونیکی ساده و مطمئن است (For confirmation, see Mazaheri and Nazem, 2009: 51). همسو با این مواد، در

---

۱. ماده ۱۲۹۲ قانون مدنی بیان می‌دارد؛ در مقابل اسناد رسمی یا اسنادی که اعتبار اسناد رسمی را دارد، انکار و تردید مسموع نیست و طرف می‌تواند ادعای جعلیت به اسناد مزبور کند یا ثابت کند که اسناد مزبور به جهتی از جهات قانونی از اعتبار افتاده است.

۲. صحت مطلب منوط به این است که عبارت «قابل استناد» مذکور در ماده را صفت «اسناد» بدانیم.

ماده ۱۲ قانون مذکور «در هیچ محکمه یا اداره دولتی نمی‌توان بر اساس قواعد ادله موجود، ارزش اثباتی «داده پیام» را صرفاً به دلیل شکل و قالب آن رد کرد».

همچنین ممکن است ایراد شود، سند عادی نیز هرچند انکارپذیر است اما قابل استناد است؛ زیرا اولاً سند است و تعریف سند بر اساس ماده ۱۲۸۴ قانون مدنی عبارت است از «هر نوشته که در مقام دعوی یا دفاع *قابل استناد* باشد» (emphasis added by the author) و ثانیاً، هرچند موضوع جعل در جعل سنتی علاوه بر سند (اعم از سند عادی و سند رسمی) می‌تواند نوشته باشد؛ اما شرط تحقق جعل در خصوص نوشته نیز آن است که قابلیت استناد داشته باشد. به عبارتی، منحصر دانستن عبارت قابل استناد به اسناد رسمی محملی ندارد و شرط قابل استناد بودن در جعل سنتی در اسناد رسمی، اسناد عادی و حتی نوشته نیز وجود دارد؛ در این راستا برخی (Mir Mohammad Sadeghi, 2023: 252) جعل را در فتوکپی اسناد به جهت قابل استناد نبودن آن‌ها قابل تحقق نمی‌دانند و نظریه مشورتی اداره کل حقوقی قوه قضاییه با شماره ۶۷۸ /۷/۹۸ نیز همسو با این دیدگاه است؛ در این میان، عده‌ای (منصورآبادی و فتحی، ۱۳۹۰، ص ۱۷۰) حتی اگر کپی یا تصویر برابر اصل شده را نیز به جهت اینکه قابلیت استناد ندارد موضوع جعل و تزویر نمی‌دانند. با پذیرش نظر اخیر شرط قابل استناد بودن در جعل سنتی نیز وجود دارد و از این حیث، جعل سنتی و جعل رایانه‌ای مشابه هستند.

علی‌رغم اشکالات فوق، ***اولاً*** در قانون تجارت الکترونیک تنها در ماده ۱۴ به عبارت «قابل استناد» اشاره شده است و مواد ۶، ۷ و ۱۲ قانون تجارت الکترونیک در خصوص ارزش اثباتی داده پیام است و نه در مورد قابل استناد بودن آن. ***دوم*** اینکه، عدم خدشه به انکارناپذیری داده ایجاد شده یکی از اوصافی است که به‌صراحت قانون‌گذار بر اساس ماده ۵۰ قانون جرائم رایانه‌ای و با نسخ ماده مذکور به موجب ماده ۶۸۵ قانون

آیین دادرسی کیفری[۱] برای قابل استناد دانستن داده ذکر کرده است و از آنجا که مقصود از انکارناپذیری را باید مسموع ندانستن انکار و تردید دانست می‌توان گفت مقصود از قابل استناد بودن در موضوع جعل رایانه‌ای قانون جرائم رایانه‌ای، قابل استناد بودن در معنای خاص آن و به‌نوعی همسنگ رسمی بودن در جعل سنتی است؛ به عبارتی می‌توان قابل استناد بودن در جعل سنتی و جعل رایانه‌ای را به دو قسم قابل استناد مطلق (اسناد رسمی در جعل سنتی و داده مطمئن) و قابل استناد مشروط (اسناد عادی در جعل سنتی و داده پیام عادی که واجد وصف مطمئن نباشد در جعل داده) تقسیم کرد و با لحاظ اینکه داده قابل استناد داده‌ای است که به انکارناپذیری آن خدشه وارد نشود، تنها داده پیام‌هایی که به‌طور مطلق قابل استناد باشند و به تعبیری واجد وصف مطمئن هستند را موضوع جعل رایانه‌ای دانست.

سوم؛ مجازات تعیین شده برای جرم جعل رایانه‌ای نیز خود نشانگر اهمیت این جرم از منظر قانون‌گذار است و نمی‌توان رفتارهای کم‌اهمیت را ذیل جرم جعل رایانه-ای قرار داد. قانون‌گذار، برای جعل سنتی در اسناد رسمی سه سال حبس تعیین کرده است و افرادی که از طریق سامانه‌های رایانه‌ای اسرار دیگری، محتویات مستهجن، تصاویر و فیلم خصوصی دیگری یا اکاذیب را منتشر می‌کنند یا مرتکب جرائمی نظیر تخریب داده، اختلال در عملکرد سامانه رایانه‌ای می‌شوند حداکثر دو سال حبس تعیین کرده است و در مقابل، برای جعل رایانه‌ای پنج سال حبس تعیین شده است و معقول نیست چنانچه شخصی تصاویر و فیلم خصوصی دیگری را منتشر کند، با دو سال حبس مواجه باشد، اما چنانچه صفحه‌ای در فیس بوک با نام و تصویر عادی دیگری ایجاد کند حداکثر مجازات پنج سال حبس باشد.

---

۱. ماده ۶۸۵ قانون آیین دادرسی کیفری اشعار می‌دارد: «چنانچه داده‌های رایانه‌ای توسط طرف دعوی یا شخص ثالثی که از دعوی آگاهی ندارد، ایجاد یا پردازش یا ذخیره یا منتقل شود و سامانه رایانه‌ای یا مخابراتی مربوط به نحوی درست عمل کند که به صحت و تمامیت، اعتبار و انکارناپذیری داده‌ها خدشه وارد نشود، قابل استناد است».

چهارم؛ در صورت تردید نسبت به اینکه آیا موضوع جعل داده، داده پیام مطمئن یا هر داده پیام دارای ارزش اثباتی است در صورت حصول تردید و سرگردانی برای برون رفت از آن ناگزیر از مراجعه به اصول حقوقی اعم از نوشته و نانوشته هستیم. در خصوص موضوع نوشتار حاضر نیز اصول و قواعد حقوقی و فقهی نظیر اصل برائت، قاعده درا، اصالت الاباحه، اصل قانونی بودن جرم و مجازات و نتیجه آن یعنی تفسیر مضیق و به نفع متهم قوانین کیفری در خصوص قلمرو مصادیق جعل رایانه‌ای راهگشاست.

پنجم؛ قیودی که قانون‌گذار در مورد داده پیام مطمئن به کار برده است یعنی به نحوی معقول در برابر سوءاستفاده 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 قیود سخت‌گیرانه‌ای نیست. درهرحال، حتی اگر داده قابل استناد را داده مطمئن ندانیم، تردیدی نیست به کار بردن تمهیدات امنیتی با توجه به مواد قانونی ازجمله ماده ۶۵۵ و ۶۵۶ قانون آیین دادرسی کیفری بر قابل استناد بودن ادله الکترونیک مؤثر است. حتی در مورد ارزش اثباتی داده پیام، ولو اینکه متصف به وصف مطمئن نباشد با عنایت به ماده ۱۳ قانون تجارت الکترونیک ارزش اثباتی داده پیام‌ها با توجه به عوامل مطمئنه ازجمله تناسب روش‌های ایمنی به کار گرفته شده با موضوع و منظور مبادله تعیین می‌شود.

از طرفی، به کار بردن تدابیر امنیتی بر قابل اطمینان بودن داده مؤثر است و قابل‌اطمینان بودن داده در ارزش اثباتی و قابل استناد بودن داده تأثیرگذار است که این مفهوم از ماده ۱۳ قانون تجارت الکترونیک و مواد دیگر قابل استنباط است. در ماده ۹ قانون نمونه آنسیترال در مورد تجارت الکترونیک ۱۹۹۶ که در خصوص قابل پذیرش بودن و ارزش اثباتی داده پیام است در ارزیابی ارزش اثباتی[1] داده پیام به قابلیت اطمینان

1 . Evidential weight.

روشی که داده پیام تولید، ذخیره یا مخابره شده است، به قابلیت اطمینان روشی که در آن یکپارچگی اطلاعات حفظ شده است و روشی که اصل ساز[1] (منشأ اصلی داده پیام) شناسایی می‌شود و عوامل مرتبط دیگر اشاره شده است.

این دیدگاه از لحاظ عملی نیز موجه است؛ زیرا چنانچه ایجاد داده‌ای که به‌خودی‌خود فاقد اعتبار و با انکار نیازمند احراز و اثبات است یا تمهیدات امنیتی در آن رعایت نشده است را به‌عنوان موضوع جرم جعل رایانه‌ای تلقی نماییم بسیاری از رفتارهای اشخاص به دلیل اینکه ایجاد آن‌ها به سهولت و بدون صرف هزینه، وقت و داشتن تخصص صورت می‌گیرد مشمول وصف کیفری با مجازات شدید قرار خواهند گرفت، درصورتی‌که حقوق کیفری استثنا است و باید استثنا بماند و مداخله کیفری حتی‌الامکان باید محدود و منحصر به مواردی باشد که بر اساس اصول جرم‌انگاری صورت گرفته باشد[2].

۱-۳-۲. اعتبار

در ماده ۶۸۵ قانون آیین دادرسی کیفری در مورد داده قابل استناد در کنار وصف «انکارناپذیری» به «اعتبار» داده‌ها اشاره شده است؛ اعتبار در سه معنای ۱- ارزش اثباتی، ۲- مقاومت در برابر انکار و تردید ۳- قابلیت استناد یا تحمیل مفاد سند در قانون به کار رفته است (Shams, 2023: 96–97). واژگان «اعتبار» و «معتبر» در مواد مختلفی از قانون مدنی و قانون تجارت الکترونیک استفاده شده است. در ماده ۱۴ قانون تجارت الکترونیک کلیه «داده پیام»هایی که به طریق مطمئن ایجاد و نگهداری شده‌اند در حکم اسناد معتبر و قابل استناد دانسته شده است و در مورد داده پیام نیز از ماده ۱۵ قانون تجارت الکترونیک قابل استنباط است که داده پیام «مطمئن» داده پیام معتبر محسوب

---

1 . Originator.

۲. بااین‌حال برخی (Salehi & Mohtaram Qalati, 2018: 182) معتقدند مقنن در تعیین مجازات تفاوتی بین جعل داده دارای ارزش اثباتی مطمئن با داده دارای ارزش اثباتی عادی قائل نشده است.

می‌شود. به همین شکل، در خصوص جعل کامپیوتری ماده ۶۸ قانون تجارت الکترونیک، قصد استفاده از داده ایجاد شده به‌عنوان داده پیام معتبر شرط تحقق جرم دانسته شده است.

در قانون مدنی نیز واژه‌های مذکور به کار برده شده است؛ وفق قانون مدنی سند به دو قسم سند رسمی و سند عادی قابل تقسیم است و سند رسمی[1] به موجب ماده ۱۲۹۰ قانون مذکور درباره طرفین و وراث و قائم‌مقام آنان «معتبر» است و «اعتبار» آن‌ها نسبت به اشخاص ثالث در صورتی است که قانون تصریح کرده باشد؛ اما بر اساس ماده ۱۲۹۱ قانون مدنی اسناد عادی در دو مورد «اعتبار» اسناد رسمی را داشته و درباره طرفین و وراث و قائم‌مقام آنان «معتبر» است. نخست آنکه طرفی که سند علیه او اقامه شده است صدور آن را از منتسب الیه تصدیق کند. در مقام مقایسه با داده، این حالت را می‌توان نظیر حالتی دانست که شخصی انتساب ایجاد یا تغییر داده به خود را تأیید کند. روشن است این حالت، قابل تطبیق با اقرار است و اعتبار نوشته از اقرار شخص گرفته می‌شود. به عبارتی اگر شخصی داده‌هایی را به مرجع قضایی ارائه کند یا حتی اسکرین شات پیام‌هایی را به مرجعی ارائه کند و طرف مقابل ارسال آن را از طرف خود تأیید کند، می‌تواند مستند حکم قرار گیرد اما پذیرش آن‌ها نه به اعتبار قابل استناد بودن داده یا اسکرین‌شات که به اعتبار اقرار منتسب‌الیه است؛ چه اگر بدون ارائه اصل داده یا اسکرین شات آن، نیز فرد مدعی ارسال داده پیام از جانب شخص ثالثی شود با تأیید اظهارات توسط ثالث می‌توان بر اساس اقرار وی حکم صادر کرد.

حالت دوم آن است که در محکمه ثابت شود که سند مزبور را طرفی که آن را تکذیب یا تردید کرده، فی‌الواقع امضا یا مهر کرده است. در این حالت نیز سند به‌خودی‌خود واجد اعتبار نیست و با انکار طرف مقابل، نیازمند بررسی توسط دادگاه و

---

۱. ماده ۱۲۸۷ قانون مدنی سند رسمی را این‌گونه تعریف می‌کند: «اسنادی که در اداره ثبت‌اسناد و املاک و یا دفاتر اسناد رسمی یا در نزد سایر مأمورین رسمی در حدود صلاحیت آن‌ها و بر طبق مقررات قانونی تنظیم‌شده باشند رسمی است».

احراز امضا یا مهر آن سند توسط منتسب‌الیه است. به جهت تفاوت بین سند عادی و سند رسمی از حیث شیوه تنظیم، اعتبار آن‌ها متفاوت است و سند رسمی معتبر است؛ درحالی‌که سند عادی، به شرحی که آمد، مشروط به اقرار طرف مقابل یا اثبات در دادگاه واجد اعتبار خواهد بود.

۱-۳-۳. صحت و تمامیت

وصف دیگری که در ماده ۶۸۵ قانون آیین دادرسی کیفری برای قابل استناد بودن به آن اشاره کرده است، عدم خدشه به صحت و تمامیت داده است؛ فصل دوم از قانون جرائم رایانه‌ای نیز با عنوان «جرائم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی» منقسم به دو مبحث با عناوین «جعل رایانه‌ای» و «تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی» است. جعل رایانه‌ای، بیشتر مرتبط با عنوان جرم علیه صحت داده و عنوان جرم علیه تمامیت داده بیشتر ناظر به جرائم تخریب و اخلال در داده و سامانه رایانه‌ای و مخابراتی است.[۱] در خصوص صحت داده پیام ماده ۱۶ قانون تجارت الکترونیک، اشعار می‌دارد هر «داده پیام» که توسط شخص ثالث مطابق با شرایط ماده (۱۱) این قانون ثبت و نگهداری می‌شود، مقرون به صحت است.

با عنایت به مطالب گفته شده چنانچه شرایط داده قابل استناد را عیناً منطبق با شرایط داده پیام مطمئن ندانیم، می‌توان معیار قابل استناد را مواردی دانست که با توجه به اصول حقوقی داده فی‌نفسه معتبر و قابلیت استناد را داشته باشد، نه اینکه اعتبار و استناد پذیری آن مستلزم بررسی و اثبات نزد قاضی یا اقرار شخصی باشد که داده به او

---

۱. البته عبارت تمامیت (Integrity) داده که در معنای موجودیت کامل و بدون تغییر «داده پیام» در بند «ه» ماده ۲ قانون تجارت الکترونیک آمده است در حالاتی از جرم جعل داده نیز رخ می‌دهد؛ چه آنکه از مصادیق تغییر داده که به‌عنوان رفتار فیزیکی جرم جعل داده در بند الف ماده ۷۳۴ ق.م.ا در کنار ایجاد داده آمده است تغییر از طریق حذف داده است و اساساً یکی از اوصاف قانون‌گذار به موجب ماده ۶۸۵ قانون آیین دادرسی کیفری برای قابل استناد بودن دادن به شرحی که خواهد آمد خدشه وارد نشدن به تمامیت داده است.

منتسب است. در این بین، با توجه به واژه‌های اعتبار و انکارناپذیری می‌توان در مورد مفهوم داده قابل استناد از معیار تشخیص مدعی و منکر استفاده کرد و در این راستا به اینکه بار اثبات بر دوش چه کسی است استفاده کرد؛ بدین شرح که داده‌ای قابل استناد است که صحت انتساب آن نیازمند اثبات نباشد و منکر انتساب باید عدم انتساب را اثبات کند؛ به عبارتی، مقصود از قابل استناد بودن در قانون جرائم رایانه‌ای آن است که داده ایجاد شده اعتباری هم‌پایه سند رسمی داشته باشد و به‌تبع آن انکارپذیر نیست؛ به عبارتی، داده‌ای که قابل استناد نیست به‌صرف انکار منتسب الیه، همانند سند عادی، اثبات صحت آن و تکلیف اثبات بر عهده طرفی است که بدان استناد می‌کند؛ اما داده قابل استناد، قابل‌انکار نیست و در مورد آن تنها می‌توان ادعای جعل مطرح کرد که طبعاً اثبات جعلی بودن آن و بار اثبات و دلیل‌آوری[1] بر عهده مدعی است. بدیهی است در این مسیر، عرف نیز کمک کننده خواهد بود. همچنین و درهرحال، همان‌گونه که پیشتر نیز اشاره شد استفاده از تمهیدات امنیتی برای قابل استناد بودن داده شرط است.

در اینجا لازم است به این مطلب اشاره شود که قابلیت استناد و ارزش اثباتی و به‌طورکلی واژه‌ها و عبارات به کار برده شده توسط قانون‌گذار می‌توانند معانی متفاوتی داشته باشد؛ برای نمونه، در مورد استناد پذیری (قابل استناد) آمده است استناد پذیری دو مفهوم را به ذهن متبادر می‌سازد؛ در مفهوم عام، مبین امکان طرح یا ورود ادله الکترونیکی به فرآیند دادرسی کیفری اعم از اینکه موردپذیرش دادگاه قرار بگیرد یا نه و مفهوم خاص‌تر، استناد پذیری به معنای «داشتن ارزش اثباتی، حجیت، انکارناپذیر بودن ادله و درواقع، قابلیت استناد آن در صدور حکم توسط قاضی پس از ارزیابی دلیل است» (Karimi, 2012: 118)؛ همچنین آمده است استناد پذیری ادله الکترونیکی «بیانگر مجموعه قواعدی است که بر اساس آن یک دلیل الکترونیکی معتبر و دارای ارزش

---

۱. اصولاً وفق ماده ۲۱۹ قانون آیین دادرسی مدنی ادعای جعل در مورد اسناد و مدارک باید همراه با ذکر دلیل باشد.

اثباتی تلقی شده و می‌تواند مبنای صدور رأی قاضی قرار گیرد» (Karimi, 2012: 118). بااین‌حال با اوصاف ذکر شده توسط مقنن برای قابل استناد دانستن داده، از یک منظر داشتن ارزش اثباتی اعم از قابل استناد بودن خواهد بود؛ بدین توضیح که حتی داده‌هایی که دارای ارزش اثباتی باشند ممکن است برای مثال انکارپذیر بوده و درنتیجه، قابل استناد در معنای خاص نباشند.

لازم به ذکر است در ماده ۶۵۶ قانون آیین دادرسی کیفری و مواد ۱، ۷، ۱۶ و ۱۸ آیین‌نامه جمع‌آوری و استناد پذیری ادله الکترونیکی نیز به واژه‌های صحت، تمامیت، اعتبار و انکارناپذیری اشاره شده است.

۲. دیگر شرایط تحقق جعل داده

در گفتار نخست، به اوصاف قانونی داده قابل استناد اشاره شد و تردیدی نیست قابل‌اطمینان بودن داده از شرایط قابل استنباط از قانون در مورد داده قابل استناد است. در این فصل، به شرایطی اشاره می‌شود که داده در آن شرایط می‌تواند قابل اطمینان و قابل استناد باشد.

۲-۱. شرایط شکلی

در این مبحث شرایط شکلی داده قابل استناد، صرف‌نظر از محتوای داده، مورد بحث قرار می‌گیرد.

۲-۱-۱. انتساب ایجاد یا تغییر داده به دیگری

انتساب داده پیام به معنای تعلق داده پیام به فرد معینی تعریف شده است (Savarai, 2021: 171–172) که از شرایط قابل‌ذکر برای جعل داده است؛ به عبارتی، داده ایجاد شده باید منتسب به شخص دیگری غیر از ایجاد کننده یا تغییر دهنده داده باشد؛ به عبارتی همانند جعل سنتی که مطابق یک قاعده مشهور در جعل «نوشته باید در مورد

خود دروغ بگوید»[1] (Turner, 2013: 375) چنانچه صرفاً حاوی اطلاعات نادرست باشد جعل سنتی محقق نیست، در جعل رایانه‌ای نیز به‌صرف بیان مطالب خلاف واقع، چنانچه مطالب منتسب به دیگری (غیر از ایجاد کننده یا تغییردهنده) نباشد، جعل داده محقق نمی‌شود؛ بنابراین چنانچه فردی برای پذیرش در شغل، مراکز علمی یا پژوهشی یا هر نهاد دیگری اطلاعات نادرست وارد کند، ازجمله اینکه معدل یا مدرک یا رشته تحصیلی خود را خلاف واقع قید کند جرم جعل داده محقق نشده است. مواد ۶۶۷ و ۶۵۶ قانون آیین دادرسی کیفری در راستای قابل انتساب بودن اطلاعات الکترونیکی پیش‌بینی شده است.

اشاره به این مطلب نیز ضروری است؛ چنانچه در ایجاد داده منتسب به خود مطلب دروغی را به دیگری نسبت دهد نیز جرم جعل رایانه‌ای محقق نمی‌شود؛ بنابراین چنانچه شخصی در پایگاه خبری که متعلق به خود اوست یا با استفاده از حساب کاربری متعلق به خود، مطالبی را به‌طور خلاف واقع به نقل از دیگری ذکر کند، نمی‌توان وی را مرتکب جعل داده دانست و موضوع قابل بررسی با جرم نشر اکاذیب رایانه‌ای است.

۲-۱-۲. معقول بودن انتساب داده جعلی به دیگری

صرف ایجاد داده یا تغییر آن، حتی اگر منتسب به دیگری باشد کافی نیست و ضروری است با لحاظ مواردی نظیر شرایط و وضعیتی که داده در آن ایجاد شده است، احراز هویت برای ایجاد داده، نحوه تغییر داده و امکان شناسایی تغییر و شخص تغییردهنده انتساب داده به شخصی که داده به نام او جعل شده است عقلایی باشد در غیر این صورت، اصولاً امکان اضرار به دیگری وجود ندارد و امکان به اشتباه انداختن افراد عادی در خصوص اینکه داده ایجاد شده را منتسب به شخص بدانند وجود ندارد و به

1. The writing must tell a lie about itself.

فرض که امکان اضرار و به اشتباه انداختن اشخاص عادی وجود داشته باشد داده ایجاد شده را به شرحی که در مبحث پیشین آمد، نمی‌توان قابل استناد دانست. بدین منظور، احراز هویت و اصالت ضروری است.

از این جهت است، اینکه در دادنامه به شماره 9309970220400891 ایجاد صفحه در فیس‌بوک به نام دیگری و بدون اجازه وی، از مصادیق بزه جعل رایانه‌ای محسوب شده است به عقیده نگارنده قابل پذیرش نیست؛ زیرا نحوه ایجاد صفحه و حساب کاربری در شبکه اجتماعی مذکور و شبکه‌های اجتماعی دیگری نظیر توییتر، تلگرام و یا ایجاد پست الکترونیک به‌سادگی و بدون اعتبار سنجی دقیق است که همین امر موجب می‌شود صرف ایجاد صفحه و تبادل و ارسال پیام با آن در حیطه جرم جعل داده قابل بررسی نباشد مگر آنکه احراز هویت و اعتبار سنجی از طرق مناسب ازجمله دریافت نشان تأیید شده[1] (تیک آبی) صورت گرفته باشد و این احراز هویت و اعتبارسنجی نیز به نحو مطمئنی صورت گرفته باشد[2]. به همین نحو، چنانچه سامانه‌ای برای درخواست اشخاص در زمینه‌های مختلف ازجمله شرکت در آزمون استخدامی یا آزمون‌های تحصیلی، اعطای تسهیلات یا تخصیص و توزیع کالا و نظایر آن ایجاد شده باشد ولی اعتبار سنجی برای احراز هویت درخواست کننده وجود نداشته باشد و شخصی با وارد کردن مشخصات دیگری ازجمله کد ملی او درخواست را به‌جای دیگری ثبت کند جرم جعل داده وجود نخواهد داشت.

همچنین به خاطر شرط موضوع بحث است که اگر شخصی آرم مؤسسه یا نهادی را در صفحه شخصی خود قرار دهد و یا آن را ذیل مطلبی که در جایی نشر می‌دهد قرار دهد، جعل داده محسوب نمی‌شود؛ زیرا انتساب داده به نحو معقول به مؤسسه یا نهاد با

---

1. Verified Badge.

۲. لازم به ذکر است که در مواردی افراد از طریق هک کردن شبکه اجتماعی دیگری، برای مخاطبین وی پیام ارسال می‌کنند که در این موارد امکان تحقق جرم جعل داده وجود دارد مشروط به اینکه سابق بر آن نیز با فرد از این طریق ارتباطی داشته باشد و از این حیث، تصور ارسال پیام از طرف شخص معقول باشد.

گذاشتن آرم ذیل سایت و یا مطلب صورت نمی‌گیرد. به‌علاوه مطابق بند (ح) ماده ۲ قانون تجارت الکترونیک یکی از شرایط «سیستم اطلاعاتی مطمئن» این است که به نحوی معقول در برابر سوءاستفاده محفوظ باشد و موارد فوق‌الذکر (ایجاد صفحه در فیس‌بوک و نظایر آن یا گذاشتن آرم نهاد ذیل صفحه یا نوشته) فاقد این شرط است. در این زمینه، علی‌رغم اینکه در ماده ۶۸ قانون تجارت الکترونیک جرم «جعل کامپیوتری» پیش‌بینی شده است اما در ماده ۶۶ قانون مذکور استفاده از علائم تجاری به صورت نام دامنه (Domain Name) و یا هر نوع نمایش بر خط (Online) علائم تجاری که موجب فریب یا مشتبه شدن طرف به اصالت کالا و خدمات شود به صورت جداگانه جرم‌انگاری و برای آن مجازات تعیین شده است.

در پایان، این مبحث لازم به ذکر است نخستین مرحله از احراز شرط قابل استناد بودن داده در معنای عام آن این است که داده منتسب به یک فرد، نهاد، منبع یا مرجع مشخص (سامانه الکترونیکی آن‌ها) باشد. منتسب بودن در جعل سنتی نیز قابل طرح است و جعل در مصادیق مذکور در ماده ۵۲۳ از کتاب تعزیرات ق.م.ا و مواد دیگر نظیر نوشته، سند، مهر، امضا و ... زمانی معنا می‌یابد که آنچه ایجاد یا تغییر کرده است به شخص یا اشخاص یا نهاد و مراجعی منتسب باشد. بر این اساس، بدیهی است اگر شخصی اقدام به ارائه اطلاعات نادرست در فضای مجازی کند و اطلاعات به هیچ شخص یا نهادی منتسب نباشد، جعل رایانه‌ای واقع نشده است و به بیان دیگر، شرط بند نخست این مبحث محقق نشده است. نوشته و سند با امضا ذیل آن و مشخصات ذکر شده در متن منتسب به طرفین است و در مورد جعل رایانه‌ای مواردی مانند استفاده از سیم‌کارت دیگری می‌تواند انتساب داده را به دیگری نشان دهد. از طرف دیگر، فقدان شرایط و اوصافی که قانون‌گذار برای داده قابل استناد بدان اشاره کرده است به معنای فقدان شرط معقول بودن انتساب داده به دیگری است.

۲-۱-۳. امکان عقلایی فریفتن انسان عادی

در این مبحث، به این سؤال پاسخ داده می‌شود که آیا در جعل داده، شباهت کامل یا نسبی شرط تحقق بزه است یا امکان به اشتباه انداختن دیگری برای تحقق جرم کافی است. به نظر نگارنده در جرم جعل رایانه‌ای، امکان به اشتباه انداختن افراد عادی کافی و به عبارت بهتر، شرط تحقق جرم است. در جعل سنتی نیز علی‌رغم عدم تصریح قانون‌گذار، برخی احتمال معقول به اشتباه انداختن و «مشتبه کردن» افراد متعارف و معمولی که مورد تقلبی را به‌جای اصل بگیرند شرط می‌دانند (Mir Mohammad Sadeghi, 2023: 257; Barani, 2021: 28). همان‌گونه که آمده است، جرم جعل و کلاه‌برداری از این جهت که هر دو به‌نوعی تحریف حقیقت و توسل به حیله و فریب است، بسیار شبیه به هم هستند (Mir Mohammad Sadeghi, 2023: 200). حیله و فریب، امری فراتر از دروغ صرف ولو به صورت مکتوب است و تأثیر آن بر اشخاص عادی ضروری است. از این جهت است که یکی از شرایط تحقق کلاه‌برداری نیز نوعاً فریبنده بودن وسیله استفاده شده توسط مرتکب است. لذا چنانچه ساختن شی به نحوی باشد که امکان فریب یک شخص عادی وجود نداشته باشد، رفتار سازنده با جرم جعل منطبق نخواهد بود.

از طرفی، هدف مرتکب از جعل، فریب دیگری است که آن را به‌جای اصل بپذیرد. قابلیت به اشتباه انداختن دیگری و یا قابلیت اضرار به دیگری از معنای لغوی واژه قابل‌درک است. به همین شکل از *عبارت* «قابل استناد» نیز می‌توان قید امکان فریب دیگری را دریافت. چه آنکه اگر قابلیت استناد داده را نزد افراد جامعه بدانیم باید افراد متعارف را ملاک قرار دهیم و چنانچه مقصود از عبارت مذکور را اعتبار داده نزد مقام قضایی بدانیم، اصولاً باید پذیرفت که داده باید بتواند توسط یک انسان عادی نیز در بادی امر به‌عنوان داده اصلی پذیرفته شود؛ به‌علاوه، داده ایجاد شده باید واجد ارزش ذاتی برای فریب دیگری باشند و به عبارتی، چنانچه دیگر اقدامات گمراه‌کننده مرتکب

که بی‌ارتباط با داده ایجاد شده است موجب اعتماد افراد عادی باشد، برای قابل استناد بودن آن کافی نخواهد بود.

اشاره به این مطلب ضروری است که آنچه در جعل سنتی محل اختلاف است این است که آیا ضروری است که شباهت کامل یا نسبی بین آنچه جعل شده است با نمونه واقعی آن وجود داشته باشد یا اینکه امکان به اشتباه انداختن افراد کافی است؛ اما در خصوص جعل داده در بسیاری از موارد طبع و ویژگی داده و پیشرفت تکنولوژی به نحوی است که برای ایجاد داده کاملاً شبیه به داده واقعی، زمان و تجهیزات و دانش چندانی ضروری نیست و با استفاده از نرم‌افزارهای رایانه‌ای می‌توان بسیاری از داده‌ها را در زمان بسیار اندکی ایجاد کرد. درهرحال، در مواردی که یک انسان عادی یا بخش قابل‌توجهی از مردم به دلایل مختلف ازجمله سهولت ایجاد داده، تبلیغات گسترده در رسانه‌های جمعی و ... داده‌ای را، ولو کاملاً مشابه با داده واقعی، فریب‌دهنده ندانند و به عبارتی داده ایجاد شده نسبت به بخش قابل‌توجه و اکثریت مردم قابلیت استفاده به‌جای اصل را نداشته باشد، نمی‌توان جعل داده را محقق دانست.

مبنای جرم انگاری جرم جعل اعم از سنتی و رایانه‌ای، تقویت اعتماد عمومی نسبت به اشیائی است که ابزار بیان اراده هستند و البته در بحث کیفری موضوع جرم باید مورد تصریح مقنن قرار گیرد و اشیائی که موضوع جعل عرفی قرار می‌گیرند ممکن است موضوع جعل کیفری نباشند[1]؛ بدین توضیح که برخی از موارد ممکن است از دید مردم جعل محسوب شود اما به جهت اصل قانونی بودن و از این لحاظ که موضوع جرم محدود به موارد مصرح قانونی است ازنظر قانونی جعل محسوب نشود. درهرحال، باید توجه داشت که اعتماد عمومی در خصوص داده‌هایی که امکان انتساب آن‌ها به شخص

---

۱. در این راستا در دادنامه به شماره 9309970223901498 منظور از رکن ضرری جرم جعل ضرر اجتماعی است، یعنی سلب اعتماد عمومی به اسناد و نه ضرر مادی یا معنوی دانسته شده است.

خاصی به نحو معقول و متعارفی وجود ندارد سلب نمی‌شود و اساساً عموم مردم به چنین داده‌های بی‌اعتماد هستند و موضوعاً مبنای مذکور منتفی است.

۲-۲. شرایط ماهوی

علاوه بر جنبه شکلی از حیث ماهوی (محتوای داده) نیز ضروری است داده منطبق با شرایطی باشد.

۲-۲-۱. داشتن اعتبار حقوقی

در جعل سنتی، ارزش حقوقی سند و نوشته به‌عنوان یکی از شرایط تحقق جرم، بدین معنا که در روابط و موقعیت‌های حقوقی و یا روابط مالی و معاملاتی بین افراد در جامعه حسب مورد قابل استناد و واجد اثر باشد، مورد اشاره واقع شده و برخی معتقدند برخلاف شرط شباهت که محل اختلاف حقوقدانان است، شرط ارزش و اعتبار حقوقی سند و نوشته محل اتفاق است (Mansour Abadi & Fathi, 2011: 169).

چنانچه شخصی به‌حساب کاربری دیگری وارد و در قسمت توضیحاتی که شخص در مورد خود بیان کرده است تغییراتی انجام دهد، در اینکه جعل داده محقق شده است یا خیر، محل بحث و بررسی است. در اینجا، شرط انتساب مطالب تغییر داده شده به دیگری با عنایت به الزامی بودن رمز ورود محقق است. مطالبی که تغییر داده می‌شود نیز در تحقق شرط قابل استناد بودن مهم است و نمی‌توان بدون توجه به آن‌ها در این خصوص نظر داد؛ برای مثال، چنانچه شخصی روز تولد دیگری را تغییر دهد اثری بر آن مترتب نیست و به جهت غیر قابل استناد بودن داده جرم مذکور واقع نشده است؛ بااین‌حال، در این حالت با توجه به اشتراط ضرر بالقوه داده قابل استناد نخواهد بود.

ازجمله ابهامات که توسط مجمع حقوقی شورای نگهبان نیز مطرح شده است این است که قابلیت استناد نسبت به چه شخص یا مرجعی ملاک است؛ برخی (Alipour, 2021: 209, 210) با عنایت به دو معیار دعوا و دفاع بیان داشته‌اند می‌توان استناد

پذیری را در نهادهای دولتی به‌ویژه دادگاه‌ها سراغ گرفت و از این‌رو پیشنهاد اصلاح قوانین جهت تسری به پیوندهای خصوصی و حتی نزد نهادهای خصوصی طرح شده است (همان).

در ابتدا باید اشاره کرد که بین دو مفهوم قابل استناد و محلی که مرتکب قصد استفاده از داده جعلی دارد، باید قائل به تفکیک شد و تردیدی نیست قصد استفاده از داده علاوه بر مراجع قضایی و به‌طور عام‌تر مقامات و مراجع رسمی شامل اشخاص عادی نیز است[۱]. ماده ۶۸ قانون تجارت الکترونیک نیز به جعل «داده پیام» جهت ارائه به مراجع اداری، قضایی، مالی و غیره اشاره شده است. به عبارتی، همانند جعل سنتی، نمی‌توان جعل رایانه‌ای را منصرف از مواردی دانست که در بستر ارتباطات خصوصی افراد رخ می‌دهد. از آنچه گفته شد نباید تصور کرد چنانچه داده‌ای نزد اشخاص عادی یا مراجع رسمی معتبر باشد برای تحقق جرم کافی است؛ بلکه منظور از قابل استناد بودن، قابل استناد بودن نزد مراجع قضایی است و نمی‌توان جعل داده را به حالتی که صرفاً امکان فریب افراد با آن وجود دارد یا از دید یک سازمان یا نهاد قابل پذیرش بود اطلاق کرد.

تعریف ماده ۵۰ قانون جرائم رایانه‌ای از قابل استناد بودن و به‌طورکلی استفاده از عبارت قابل استناد در قانون جرائم رایانه‌ای نشانگر آن است که منظور از ماده مذکور قابل استناد بودن در مراجع قضایی است؛ این برداشت از داده قابل استناد مضیق بوده و موارد زیادی را از شمول عنوان «داده قابل استناد» و به تبع آن جعل رایانه‌ای خارج می‌کند. ازجمله اسکرین شات، رسیدهای تقلبی، تصاویر کارت‌ها و اوراق هویت از این جهت که این تصاویر در مراجع قضایی و حقوقی به‌عنوان دلیل قابلیت استفاده را ندارند قابل استناد نبوده و موضوع جرم جعل رایانه‌ای نخواهند بود.

---

۱. حتی می‌توان گفت در جعل رایانه‌ای نیازی نیست آنچه جعل شده است، برای فریب انسان باشد بلکه جعل به‌منظور فریب یک دستگاه نیز با توجه به بند ب ماده ۷۳۵ ق.م.ا کافی است.

بدیهی است صرف اینکه هدف مرتکب ارائه داده به مراجع غیر قضایی باشد، مورد را از شمول قابل استناد بودن داده در مرجع قضایی خارج نمی‌کند؛ اساساً در بسیاری از موارد جعل داده، جهت ارائه به مراجع غیر قضایی یا شخص ثالثی ایجاد می‌شود؛ برای مثال ممکن است شخصی با نفوذ به سامانه‌های موجود در دستور آزادی متهم ترخیص خودرو را به مرجع ذی‌ربط با اکانت متعلق به مراجع قضایی بدهد؛ در مورد مذکور نیز داده در مراجع قضایی قابل استناد است؛ برای مثال چنانکه محل نگهداری خودرو از تحویل آن امتناع کند می‌توان دادخواست تحویل و استرداد آن را مطرح کرد. در ماده ۱۲ قانون تجارت الکترونیک از ارزش اثباتی داده پیام در محکمه یا اداره دولتی (که غیر از محاکم است) سخن به میان آمده است و البته در ماده مذکور به اسناد و ادله اثبات دعوا اشاره دارد که طبیعتاً ادله اثبات دعوا در مراجع قضایی مطرح است و سند نیز به‌عنوان یک دلیل اثبات در حقوق مطرح است. ماده ۱۴ قانون مذکور نیز به قابل استناد در مراجع قضایی و حقوقی اشاره دارد.

۲-۲-۲. قابلیت اضرار (ضرر بالقوه)

در خصوص قابلیت اضرار بالقوه یا بالفعل برخی معتقدند با توجه به وجود شرط بنیادین قابلیت استناد نیازی به‌شرط مذکور نیست (Alipour, 2021: 209) و همچنین بیان شده است جعل رایانه‌ای یک بزه مطلق است و در جعل رایانه‌ای موضوع ماده ۶۸ قانون تجارت الکترونیک نیز حتی احتمال ضرر بالقوه شرط تحقق جرم نیست (Ghafoori Pour Kermani, 2012: 81)؛ اولاً شرط ضرر و زیان بالقوه و مطلق دانستن جرم متناقض نیست (For a dissenting opinion, see Ghafoori Pour Kermani, 2012: 83–84). ولی ضرر بالقوه جزء شرایط و اوضاع‌واحوال جرم و نه نتیجه مجرمانه است؛ به عبارتی، این جرم از جرائم مطلق است؛ همچنین نمی‌توان پذیرفت که مرتکب باید علاوه بر علم و عمد در عمل ارتکابی باید نتیجه عمل را نیز قصد کرده باشد و

ایجاد یا تغییر داده‌ها را اراده کرده باشد (For a dissenting opinion, see Gerayeli, 2010: 170). مقصود از ضرر، ضرر مادی و غیرمادی است.

۲-۳. تحلیل مصادیق مرتبط

البته باید اذعان کرد که معیارهای رسمی بودن سند روشن است و در مقابل، معیار و مصداق داده مطمئن عینی نیست و در تشخیص مصداق امکان اختلاف وجود دارد. بااین‌حال، یکی از ایراداتی که برخی به ماده ۵۰ قانون جرائم رایانه‌ای وارد می‌سازند مشخص نبودن بار اثبات «صحت و تمامیت، اعتبار و انکارپذیری داده» است و به عبارتی این مطلب که اصل بر عملکرد صحیح سامانه‌های رایانه‌ای است و خلاف آن باید توسط طرف مقابل اثبات شود یا اینکه به‌صرف انکار عملکرد درست رایانه از سوی شخص استناد کننده باید درستی عملکرد را اثبات کند (Elsan & Manouchehri, 2018: 38)؛ در این راستا بیان شده است (Qarajehlu, 2007, cited in Elsan & Manouchehri, 2018: 39)؛ مفهوم مخالف ماده ۵۰ قانون جرائم رایانه‌ای نشانگر داده‌های رایانه‌ای دارای ارزش نیستند، مگر شرایطی در آن‌ها رعایت شود و به‌عبارت‌دیگر، اصل بر عدم اعتبار آن‌ها است که طبیعتاً اثبات قابل استناد بودن آن‌ها بر عهده استناد کننده خواهد بود. در این راستا، در صورت تردید در اینکه داده ایجاد شده توسط متهم قابل استناد است یا خیر با توجه به اینکه اصل بر برائت است باید آن را غیر قابل استناد بدانیم.

درواقع اگر ادله الکترونیکی فاقد شرایط و ضوابط قانونی باشد و این فقدان موجب باشد به اصالت و تمامیت ادله خلل وارد شود، هرچند قاضی نمی‌تواند بر مبنای دلیل الکترونیک حکم صادر کند، اما می‌تواند وفق ماده ۱۶۲ قانون مجازات اسلامی به‌عنوان اماره قضایی مورد استناد قرار گیرد مشروط به اینکه همراه با قرائن و امارات دیگر موجب علم قاضی شود (Delkhoon Asl, Goldouzian, & Kalantari, 2023: 28).

همچنین زمانی که از قابل استناد بودن داده سخن گفته می‌شود، قابلیت استناد به آن در همان حالت داده و نه مثلاً با پرینت گرفتن و تبدیل آن به نوشته یا سند فیزیکی است.

الف. شبکه‌های اجتماعی و پست الکترونیک

درصورتی‌که حساب کاربری با نام و نام خانوادگی و تصویر دیگری بدون احراز هویت مناسب و به‌سادگی صورت گرفته باشد نظیر ایجاد صفحه در فیس‌بوک و اینستاگرام با نام و تصویر دیگری یا ایجاد پست الکترونیک در گوگل یا یاهو با نام دیگری، چنین اقدامی و ارسال مطلب از طریق حساب کاربری ایجاد شده، جعل داده نخواهد بود اما چنانچه علاوه بر مشخصات شخص با شماره تماس متعلق به دیگری اقدام به ایجاد حساب کاربری شده باشد و کد احراز هویت ارسال شده باشد و حساب کاربری ایجاد شده مشخص باشد بر روی خط متعلق به دیگری فعال شده است و از آن طریق مبادرت به ارسال پیام کند جعل داده به خاطر فقدان شرط انتساب معقول محقق نشده است.

با عنایت به مطالب فوق در مورد جعل رایانه‌ای، باید قائل به این بود که امکان معقول به اشتباه انداختن افراد متعارف برای تحقق جرم شرط است. بر این اساس، در مواردی نظیر ایجاد حساب کاربری در بسیاری از شبکه‌های اجتماعی با نام افراد دیگر، به‌ویژه افراد مشهور موجب تلقی افراد جامعه در خصوص اینکه صفحات توسط آن افراد ایجاد شده است نیست. حتی اگر شباهت کامل بین داده ایجاد شده با داده واقعی وجود دارد؛ اما علی‌رغم این شباهت، مردم عادی اعتمادی به داده ایجاد شده ندارند. لازم به ذکر است صرف ایجاد حساب کاربری مثلاً در ایتا، سروش و ... با تصویر و مشخصات هویتی دیگری حتی با استفاده از سیم‌کارت دیگری جعل داده نیست؛ زیرا ایجاد حساب کاربری داده قابل استناد و دارای ارزش حقوقی نیست و قابلیت اضرار وجود ندارد.

بنابراین اینکه گفته شده است چنانچه شخصی بیانیه‌ای به نام و امضای یکی از مسئولان عالی‌مقام منتشر کند جعل نیست؛ زیرا اشخاص متعارف آن را به‌جای اصل

نمی‌پذیرند، اما اگر به نام مسئول اداره‌ای عرضه شود حتی اگر شباهتی نباشد امکان به اشتباه افتادن وجود دارد (Amirian Farsani & Hosseini, 2019: 65)، چنانچه مقصود این باشد که جعل واقع شده است از این جهت که قابلیت انتساب معقول داده به دیگری وجود ندارد قابل پذیرش نیست.

ب. اسناد و نوشته‌ها

مواردی نظیر ایجاد رسید بانکی با نرم‌افزار رسید ساز، گذاشتن آرم یک سازمان ذیل یک صفحه، گذاشتن نماد اعتبار الکترونیک ذیل صفحه خود و ایجاد اسکرین‌شات یا زمانی که شخص فاقد گواهی‌نامه با تهیه تصویر از گواهی‌نامه دیگری و تغییر آن با نشان دادن تصویر تغییر داده شده به مأمور راهنمایی رانندگی بخواهد خود را شخص دارای گواهی‌نامه جلوه دهد یا حالتی که شخصی برای جلب اعتماد و فریب دیگری در فضای مجازی تصویر کارت ملی، کارت خودرو، قولنامه و نظایر آن که به صورت جعلی ایجاد شده است ارسال کند، موضوع قابل تطبیق با جعل رایانه‌ای نیست. در موارد مذکور داده قابل استناد نیست و قابلیت انتساب معقول وجود ندارد و فاقد ارزش حقوقی است. همچنین اکثریت مردم با توجه به امکان عودت وجه به‌حساب مبدأ یا اینکه از وجود رسید ساز جعلی اطلاع دارند به‌صرف نشان دادن تصویر رسید اعتماد نمی‌کنند؛ به عبارتی در این موارد که شباهت به‌طور کامل وجود دارد نیز امکان به اشتباه انداختن یک انسان عادی و متعارف را ندارد و نمی‌توان جعل داده را محقق دانست.

در خصوص مدارک هویتی که بعضاً فایل اسکن شده آن مورد درخواست برخی از مراجع است، معمولاً نزد آن مراجع اعتباری کافی نداشته و اصل آن متعاقباً درخواست و از مراجع ذی‌ربط، استعلام می‌شود؛ بنابراین چنانچه شخصی برای استخدام در سایت مربوطه پس از اسکن تصویر مدرک تحصیلی در معدل تغییری ایجاد کند و تصویر همراه با تغییر را در سامانه مربوطه بارگذاری کند، با توجه به اینکه برای استخدام در یک نهاد دولتی تصویر مدرک تحصیلی اعتبار لازم را نداشته و برای انتساب آن به مرجع

صادرکننده ارزش کافی ندارد جعل داده رخ نداده است. ضمن اینکه از این جهت که ایجاد داده، منتسب به خود شخص است نمی‌توان جعل رایانه‌ای را متصور دانست.

همچنین تهیه تصویر از سند و تغییر در آن و ارسال به دیگری جعل داده و استفاده از آن محسوب نمی‌شود. این حالت نظیر تغییر در کپی یک سند و استفاده از آن است که نمی‌توان رفتار را جعل سنتی محسوب کرد. اینکه در قسمت دوم بند «ت» ب ماده ۳۸ قانون احکام دائمی برنامه‌های توسعه کشور مصوب ۱۳۹۵ که به قوه قضائیه اجازه داده شده است اسناد و اوراق پرونده‌های قضائی را که نگهداری سوابق آن‌ها ضروری است به اسناد الکترونیکی تبدیل و سپس نسبت به امحای آن‌ها اقدام کند، اطلاعات و اسناد تبدیلی را در کلیه مراجع قضائی و اداری دارای سندیت و قابل استناد دانسته است؛ از این جهت که تبدیل اسناد فیزیکی و تبدیل آن به اسناد الکترونیکی توسط مرجع رسمی و با ضوابط مشخص شده انجام می‌شود متفاوت با حالت مورد بحث است و بدیهی است، صرف اینکه شخصی رأساً سندی را به صورت الکترونیکی تبدیل کرد در مراجع قضایی تصویر ارائه شده فاقد اعتبار خواهد بود. در اینجا اشاره به این نکته لازم است که در مواردی که یک نهاد یا سازمان از طریق تهیه تصویر از مدارک آن را از طریق سامانه پیش‌بینی شده برای ارگان دیگر ارسال کند، موضوع می‌تواند قابل بررسی با جعل داده باشد؛ برای مثال، اینکه برگه‌های نیابت توسط دادسرای مجری نیابت اسکن و از طریق سامانه مدیریت پرونده قوه قضائیه برای دادسرای معطی نیابت ارسال شود، یا اینکه اوراق پرونده توسط مرجع انتظامی اسکن و برای مرجع قضایی ارسال می‌شود داده‌های ایجاد شده به دلایلی نظیر مرجع تهیه‌کننده و سامانه که در مقابل سوءاستفاده به نحو معقولی مصون است و انتساب معقول داده به مرجع تهیه‌کننده قابلیت استناد را دارد. به همین شکل، مواردی نظیر ورود به سامانه قضایی و ایجاد و ارسال دستور قضایی از طریق آن، ارسال پیام با استفاده از سیم‌کارت دیگری به جهت منتسب کردن مطلبی به وی، قابل تطبیق با جرم جعل رایانه‌ای است.

برخی (Alipour, 2021: 211) با قابل استناد دانستن امضای دیجیتال، با بیان اینکه امضای الکترونیکی ساده همان امضای محیط کاغذی است که با اسکن روی متن (داده) گذاشته می‌شود، امضای الکترونیکی را نیز داده که تغییر آن جعل رایانه‌ای است دانسته و معتقدند امضا در محیط فیزیکی همواره دارای اعتبار است، اما در فضای سایبر نیاز است که امضای الکترونیکی مطمئن و اصیل باشد (Alipour, 2021: 212)؛ درهرحال، در مواردی که شخصی امضا دیگری را اسکن و ذیل نوشته‌ای قرار دهد موضوع منطبق بر جعل رایانه‌ای نیست؛ زیرا انتساب آن به دیگری به نحو معقولی وجود ندارد و تمهیدات امنیتی در آن رعایت نشده است؛ اما در حال اخیر چنانچه شخص سند ایجاد شده را با استفاده از حساب کاربری متعلق به دیگری در سامانه‌ای پیش‌بینی شده بارگذاری کند، با عنایت به تحقق قید اخیر موضوع می‌تواند با جعل رایانه‌ای قابل‌بررسی باشد.

ج. تصویر و فیلم

در خصوص دیپ فیک برخی با پذیرش احتمال انطباق جعل رایانه‌ای با دیپ فیک، معتقدند ازنظر تحقق عنصر مادی با این اشکال جدی مواجه است که داده‌های موردنیاز در فناوری دیپ فیک، یعنی صدا و تصویر قبلی، واقعی است جعل رایانه‌ای تغییر یا ایجاد داده‌های قابل استناد است، به‌گونه‌ای که صدا و تصاویر واقعی را نمی‌توان از مصادیق داده دانست مگر اینکه تفسیر موسع صورت گیرد (Shiri, 2022: 160) برخی جعل عمیق را منطبق با نشر اکاذیب رایانه‌ای، هتک حیثیت از طریق تغییر فیلم دیگری و قذف (Ehsanpour & Ommi, 2022: 6-7) دانسته‌اند و در مورد تطبیق این رفتار با جعل رایانه‌ای مورد بررسی واقع نشده است.

برخی (Salehi & Qalaati, 2018: 168) معتقدند کلیه داده‌های صوتی، تصویری و یا رمزی، ممکن است دارای ارزش اثباتی و قابل استناد باشند و موضوع جرم جعل واقع شوند و به عبارتی داده قابل استناد را اعم از داده به صورت نوشته و غیر آن

می‌دانند. همچنین، به عقیده برخی (Savarai, 2014: 87) با توجه به قانون تجارت الکترونیک نظام حقوقی ایران قلمرو بسیار وسیعی از اسناد الکترونیکی را پذیرفته است و چنانچه اطلاعات در قالب صدا و تصویر نیز باشد می‌تواند مشمول سند الکترونیک باشد (Savarai, 2014: 88). لازم به ذکر است، ممکن است داده‌ای که در گذشته یا حال قابل استناد است، در آینده با توجه به تغییر شرایط غیر قابل استناد باشد. ازجمله آنکه به دلیل پیشرفت تکنولوژی به‌ویژه در حوزه هوش مصنوعی ممکن است در آینده محاکم و دادسراها بسیاری از داده‌ها را ازجمله فایل صوتی حاوی صدای دیگری، به جهت سهولت جعل عمیق قابل استناد ندانند.

فرجام سخن

مبحث نخست از فصل دوم قانون جرائم رایانه‌ای به «جعل رایانه‌ای» اختصاص و در ماده ۶ قانون مذکور بزه موصوف را «تغییر یا ایجاد داده‌های قابل استناد یا ایجاد یا واردکردن متقلبانه داده به آن‌ها» و «تغییر داده‌ها یا علائم موجود در کارت‌های حافظه یا قابل‌پردازش در سامانه‌های رایانه‌ای یا مخابراتی یا تراشه‌ها یا ایجاد یا وارد کردن متقلبانه داده‌ها یا علائم به آن‌ها» محسوب کرده و برای آن مجازات تعیین کرده است؛ صرف‌نظر از اشکال شکلی ماده مذکور، قابل استناد بودن شرط بنیادین تحقق جعل رایانه‌ای است.

مفهوم داده قابل استناد چندان روشن نیست؛ بااین‌حال، می‌توان با استفاده از قانون تجارت الکترونیک گفت هر آنچه بتوان آن را داده پیام مطمئن دانست، قابلیت استناد را داشته و می‌تواند موضوع جعل داده قرار بگیرد و برخلاف جعل سنتی که جعل می‌تواند در اسناد عادی که انتساب آن به اشخاص ایجاد کننده می‌تواند محل تردید جدی باشد و اساساً انتساب آن به فرد با انکار وی نیازمند اثبات است؛ جعل رایانه‌ای صرفاً در مورد داده‌هایی که انتساب آن از قوت و اعتبار کافی همسان اسناد رسمی برخوردار است امکان‌پذیر است. این نکته که داده قابل استناد همان داده پیام مطمئن است، از

یک‌سو از تصریح ماده ۱۴ قانون تجارت الکترونیک به اینکه داده پیام مطمئن، قابل استناد است و از سوی دیگر، از این جهت که داده پیام مطمئن بر اساس ماده ۱۵ قانون تجارت الکترونیک انکارناپذیر است و از اوصاف داده قابل استناد، وفق ماده ۶۸۵ قانون آیین دادرسی کیفری، انکارناپذیری است قابل استنباط است. چنانچه برداشت فوق را نپذیریم تردیدی نیست رعایت تدابیر امنیتی که به‌نوعی شالوده تعریف داده پیام مطمئن نیز است برای قابل استناد دانستن داده ایجاد شده شرط است. مفاهیم انکارناپذیری، اعتبار و تمامیت و صحت که در قانون ذکر شده است این برداشت را تقویت می‌کند.

از طرفی با استفاده از مفهوم داده قابل استناد در معنای موسع واژه، شرایط جعل سنتی و اصول حقوقی می‌توان شرایط شکلی و ماهوی انتساب داده به دیگری به نحو معقول، داشتن ارزش حقوقی، قابلیت فریب اشخاص عادی، احتمال ضرر بالقوه برای تحقق جعل رایانه‌ای ذکر کرد. ازاین‌روست که صرف ارسال پیام از حساب کاربری دیگری را نباید جعل داده و استفاده از آن دانست؛ زیرا جلوه دادن خود به‌جای دیگری به‌نحوی‌که داده ارسال شده به‌طور معقولی به شخص یا مرجعی خاص قابل انتساب باشد، واجد اهمیت است؛ به همین نحو شرط است محتوای ایجاد شده واجد ارزش و به صورتی باشد که ضرر اعم از مالی و غیرمالی ازجمله ضرر حیثیتی هرچند به صورت بالقوه به دیگری وارد کند و این ضرر آن‌قدر ناچیز نباشد که در نظر عرف قابل‌اغماض باشد.

با توجه به مطالب فوق، مواردی نظیر ایجاد پست الکترونیک با نام و نام خانوادگی دیگری و یا حساب کاربری در شبکه‌های مختلف اجتماعی، مشروط به اینکه احراز هویت به نحو مناسب صورت نگرفته شود، ایجاد رسید بانکی با رسید ساز درج امضای دیگری ذیل مطلب یا نوشته، گذاشتن ارم مؤسسه یا اداره ذیل یک مطلب قابل انطباق با جرم جعل رایانه‌ای نیست.

منابع

احسان پور، سیدرضا؛ امی، احمد (۱۴۰۱). جرائم «فناوری جعل عمیق» از منظر فقه و حقوق کیفری، *فقه جزای تطبیقی*، ۲(۴) ۲-۹.. Doi: 10.22034/jccj.2022.368844.1124

امیریان فارسانی، امین؛ محمد حسینی، حجت (۱۳۹۸). *حقوق جزای اختصاصی رایانه‌ای*، تهران: قانون یار.

بابایی، جواد (۱۴۰۱). *جرائم رایانه‌ای و آیین دادرسی حاکم بر آن*. تهران: قوه قضائیه.

بارانی، محمد (۱۴۰۰). *جعل و تزویر در قانون و رویه قضایی ایران*، تهران: مرکز مطبوعات و انتشارات قوه قضائیه.

ترکی، غلام عباس (۱۳۸۹). بررسی مصادیقی از جعل رایانه‌ای، *مجله دادرسی*، ۸۳، ۳۲-۳۵.

دل‌خون اصل، رامین، گلدوزیان، ایرج و کلانتری، کیومرث (۱۴۰۱). مطالعه تطبیقی ارزش اثباتی ادله الکترونیکی در فرآیند دادرسی کیفری در نظام حقوقی ایران و فرانسه .*فصلنامه مطالعات حقوقی فضای مجازی*، ۱(۴)، ۱۶-۳۲.

رباطی، مهسا؛ محسنی، سعید؛ قبولی درافشان، سید محمدمهدی (۱۳۹۶). عدم قابلیت استناد بطلان در شرکت‌های تجاری. *مطالعات حقوقی*، ۹(۴)، ۱۰۹-۱۳۰. DOI: 10.22099/jls.2018.24736.2322

روح‌بخش، فرزاد؛ حیدری، سیروس؛ رضایی، علی؛ مبین، حجت (۱۴۰۱). دادخواست الکترونیکی: ماهیت و چالش‌های ناشی از ثبت آن. *مطالعات حقوقی*، ۱۴(۲)، ۱۲۹-۱۷۳. DOI: 10.22099/jls.2021.38758.4129

السان، مصطفی؛ منوچهری، محمدرضا (۱۳۹۷). ارزیابی اصالت ادله الکترونیکی و ارزش اثباتی آن‌ها. *مطالعات حقوقی*، ۱۰(۲)، ۲۹-۵۲. doi: 10.22099/jls.2018.28058.2765

ساورایی، پرویز (۱۳۹۳). تحلیل حقوقی سند الکترونیک، *تحقیقات حقوقی*، ۶۵، ۸۳-۱۰۷.

ساورایی، پرویز (۱۴۰۰). تحلیل حقوقی جنبه‌های ثبوتی و اثباتی انتساب داده پیام در قانون تجارت الکترونیک ایران .*تحقیقات حقوقی*، ۹۳، ۱۶۹-۱۹۱. Doi: 10.29252/jlr.2021.220345.1828

شمس، عبدالله (۱۴۰۱). *ادله اثبات دعوا*، تهران: دراک.

شیری ورنامخواستی، عباس (۱۴۰۱). دیپ فیک یا همانندسازی صوتی یا تصویری غیرواقعی در حقوق کیفری، *تحقیقات حقوقی*، ۹۹ (ویژه‌نامه حقوق و فناوری)، ۱۴۳-۱۶۸. Doi: 10.52547/jlr.2023.230618.2451

صالحی، محمد خلیل، قلاتی ایمان (۱۳۹۷)، گستره و ویژگی‌های داده‌های مجعول رایانه‌ای در حقوق ایران، *پژوهشنامه حقوق کیفری*، ۱۷، ۱۶۱-۱۸۵.Doi: 10.22124/jol.2018.6728.1283

العارضی، فرقد عبود (۲۰۱۲). جریمة التزویر الالکترونی-دراسة مقارنة. *مجلة الکوفة للعلوم القانونیة والسیاسیة*، ۱(۱۳).

عالی‌پور، حسن (۱۴۰۰). *حقوق کیفری فناوری اطلاعات*، تهران: خرسندی.

عزیزی، امیرمهدی (۱۳۹۸). *حقوق کیفری جرائم رایانه‌ای*، تهران: مجد.

غفوری پور کرمانی، ارسلان (۱۳۹۱). مطالعه تطبیقی جعل رایانه‌ای در حقوق کیفری ایران و کنوانسیون جرائم تبادل اطلاعات با جعل سنتی، به راهنمایی حسن پوربافرانی، پایان‌نامه کارشناسی ارشد، دانشگاه اصفهان، دانشکده اقتصاد و علوم اداری.

فرشاسعید، پرویز؛ جلالی، محمود؛ گودرزی، مهناز (۱۴۰۰). ضرورت تدوین کنوانسیون بین‌المللی حملات سایبری. *مطالعات حقوقی*، ۱۳(۱)، ۲۰۵-۲۳۰. Doi: 10.22099/jls.2021.33031.3370

قناد، فاطمه (۱۳۹۰). جعل در بستر فناوری‌های اطلاعات و ارتباطات. *آموزه‌های حقوق کیفری*، دوره جدید(۲)، ۶۳-۸۸.

کریمی، محسن (۱۳۹۱). جمع‌آوری و استناد پذیری ادله الکترونیکی در حقوق کیفری ایران، به راهنمایی حسنعلی مؤذن‌زادگان، پایان‌نامه کارشناسی ارشد، دانشگاه علامه طباطبائی، دانشکده علوم سیاسی.

گرایلی، محمدباقر (۱۳۸۹). بررسی جعل و تخریب و اخلال رایانه‌ای. *آموزه‌های حقوق کیفری*، ۱۴، ۱۵۹-۱۸۸.

محمد نسل، غلامرضا (۱۳۹۲). *حقوق جزای اختصاصی جرائم رایانه‌ای*، تهران: میزان.

محمدی فردویی، عطا اله (۱۳۹۷). بررسی جزایی عناصر بزه جعل رایانه‌ای در حقوق ایران. *قانون یار*، ۲(۸)، ۴۵۹-۴۷۶.

مرکز پژوهش‌های مجلس شورای اسلامی (۱۴۰۰). اظهارنظر کارشناسی درباره لایحه جرائم رایانه‌ای. https://sid.ir/paper/803792/fa

مظاهری، رسول؛ ناظم، علیرضا (۱۳۸۷). ارزش اثباتی داده پیام و امضای الکترونیکی. *نامه مفید*، ۷۰، ۳۹-۵۸.

منصورآبادی، عباس؛ فتحی، محمدجواد (۱۳۹۰). موضوع جعل و تزویر، *تحقیقات حقوقی*، ۱۴(۵۳)، ۱۴۷-۱۸۲.

مؤذن زادگان، حسنعلی؛ سلیمان دهکردی، الهام؛ یوشی، مهشید (۱۳۹۴). حفظ صحت و استناد پذیری ادله الکترونیک با استفاده از بیومتریک و رمزنگاری، *پژوهش حقوق کیفری*، ۱۲، ۶۹- ۹۸. Doi:https://doi.org/10.22054/jclr.2015.1782

مؤذن زادگان، حسن علی؛ شایگان، محمد رسول (۱۳۸۸). استناد پذیری و تحصیل ادله الکترونیکی در حقوق کیفری ایران. *دیدگاه‌های حقوق قضائی*، ۴۸، ۷۷-۱۰۲.

میرمحمد صادقی، حسین (۱۴۰۲). *جرائم علیه مصالح عمومی کشور*، تهران: میزان.

References

Al-Ardi, F. (2012). The Crime of Electronic Forgery – A Comparative Study. *Al-Kufa Journal of Legal and Political Sciences*, 1(13). [In Arabic].

Alipour, H. (2021). *Criminal Law of Information Technology*, Tehran: Khorsandi. [In Persian].

Amirian Farsani, A; Hosseini, H. (2019). *Specialized Computer Criminal Law*, Tehran: Ghanoun Yar. [In Persian].

Azizi, A. M. (2019). *Criminal Law of Cyber Crimes*, Tehran: Majd. [In Persian].

Babaei, J. (2022). *Computer Crimes and the Governing Procedure*. Tehran: Judiciary. [In Persian].

Barani, M. (2021). *Forgery and Falsification in Iranian Law and Judicial Practice*, Tehran: Judiciary Press and Publications Center. [In Persian].

Delkhoon Asl, R., Goldouzian, I., & Kalantari, K. (2023). A comparative study of the probative value of electronic evidence in criminal proceedings in the legal system of Iran and France. *Quarterly Journal of Cyberspace Legal Studies*, 1(4), 16–32. [In Persian]. Doi: https://doi.org/10.30495/cyberlaw.2023.698991

Ehsanpour, SR; Ommi, A. (2022). Deepfakes Crimes from the Perspective of Jurisprudence and Criminal Law. *Comparative Criminal Jurisprudence*, 2(4), 2–9. [In Persian]. Doi: 10.22034/jccj.2022.368844.1124

Elsan, M; Manouchehri, M (2018). Evaluation of the Authenticity of Electronic Evidence and Their Probative Value. *Legal Studies*, 10(2), 29-52. [In Persian]. Doi: 10.22099/jls.2018.28058.2765

Farshasaeed, P.; Jalali, M.; Goudarzi, M. (2021). The Necessity of Drafting an International Convention on Cyber Attacks. *Legal Studies*, 13(1), 205–230. [In Persian]. Doi: 10.22099/jls.2021.33031.3370

Gerayeli, Mohammad Baqer (2010). A Study on Computer Forgery, Destruction, and Disruption. *Criminal Law Teachings*, 14, 159-188. [In Persian].

Ghafoori Pour Kermani, A. (2012). A Comparative Study of Computer Forgery in Iranian Criminal Law and the Convention on Cybercrime Compared to Traditional Forgery. *M.A. Thesis, University of Isfahan, Faculty of Economics and Administrative Sciences*. [In Persian].

Ghanad, F. (2011). Forgery in the Context of Information and Communication Technologies. *New Series of Criminal Law Teachings*, (2), 63-88. [In Persian].

Harrell, E. (2019). *Victims of identity theft, 2016: Bulletin*.

Harrell, E. (2019). *Victims of identity theft, 2016: Bulletin*.

Islamic Parliament Research Center (2021). Expert Opinion on the Draft Bill on Cyber Crimes. https://sid.ir/paper/803792/fa [In Persian].

Karimi, M. (2012). Collection and Admissibility of Electronic Evidence in Iran's Criminal Law. *M.A. Thesis, Allameh Tabataba'i University, Faculty of Political Science*. [In Persian].

Mansour Abadi, A.; Fathi, M. J. (2011). The Subject of Forgery and Falsification. *Legal Research*, 14(53), 147-182. [In Persian].

Mazaheri, R.; Nazem, A. (2009). Probative Value of Data Messages and Electronic Signatures. *Nameh Mofid*, 70, 39-58. [In Persian].

Mir Mohammad Sadeghi, H. (2023). *Crimes against the country's public interests*. Tehran: Mizan. [In Persian].

Moazenzadegan, H. A.; Shayegan, M. R. (2009). Admissibility and Collection of Electronic Evidence in Iranian Criminal Law. *Legal Judicial Views*, 48, 77-102. [In Persian].

Moazenzadegan, H. A.; Soleyman Dehkordi, E.; Youshi, M. (2015). Preserving the Integrity and Admissibility of Electronic Evidence Using Biometrics and Cryptography. *Criminal Law Research*, 12, 69–98. [In Persian]. Doi:https://doi.org/10.22054/jclr.2015.1782

Mohammad Nasl, G. (2013). *Specialized Criminal Law of Cyber Crimes*, Tehran: Mizan. [In Persian].

Mohammadi Ferdouei, A. (2018). Criminal Analysis of the Elements of Computer Forgery in Iranian Law. *Ghanoun Yar*, 2(8), 459-476. [In Persian].

Robati, M.; Mohseni, S.; Ghabouli Dorafshan, S. M. (2018). Non-Attributability of Invalidity in Commercial Companies. *Legal Studies*, 9(4), 109–130. [In Persian]. Doi: 10.22099/jls.2018.24736.2322

Rouhbakhsh, F.; Heydari, S.; Rezaei, A.; Mobin, H. (2022). Electronic Petition: Nature and Challenges Arising from Its Registration. *Legal Studies*, 14(2), 129–173. [In Persian]. doi: 10.22099/jls.2021.38758.4129

Sadiku, M. N. O., Musa, S. M., & Nelatury, S. R. (2017). Digital forgery. International Journal of Advances in Scientific Research and Engineering, 3(4).

Sadiku, M. N. O., Musa, S. M., & Nelatury, S. R. (2017). Digital forgery. *International Journal of Advances in Scientific Research and Engineering*, 3(4).

Salehi, M. K.; Qalaati, I. (2018). Scope and Characteristics of Computer-Forged Data in Iranian Law, *Criminal Law Research Journal*, 17, 161-185. [In Persian]. Doi: 10.22124/jol.2018.6728.1283

Salmond, J. W. (1907). Jurisprudence, or, the theory of the law. Stevens and Haynes.

Salmond, J. W. (1907). *Jurisprudence, or, the theory of the law*. Stevens and Haynes.

Savarai, P. (2014). Legal Analysis of Electronic Documents, *Legal Research*, 65, 83-107. [In Persian].

Savarai, P. (2021). Legal Analysis of Evidentiary and Probative Aspects of Data Message Attribution in Iran's Electronic Commerce Law. *Legal Research*, 93, 169-191. [In Persian]. Doi: 10.29252/jlr.2021.220345.1828

Shams, A. (2023). *Evidence in Lawsuits*, Tehran: Derak. [In Persian].

Shiri, A. (2022). Deepfake or Unreal Audio or Video simulation in Criminal Law. *Legal Research*, 99 (Special Issue on Law and Technology), 143-168. [In Persian]. DOI: 10.52547/jlr.2023.230618.2451

Torki, G. (2010). Examination of Instances of Computer Forgery, *Dadresi Journal*, 83, 32-35. [In Persian].

Turner, J. C. (2013). *Kenny's outlines of criminal law*. Cambridge University Press.