Modern Technologies Law

University of Science and Culture

http://doi.org/10.22133/MTLJ.2022.369536.1142

Digital Forensics in Iran and English Criminal Systems

Afshar Khosravizad[1], Roohollah Sepehri[2]*, Hamideh Bababee[3]

[1] Ph. D Student in Criminal Law and Criminology, Department of Law, Naragh Branch, Islamic Azad University, Naragh, Iran

[2] Assistant Professor, Department of Law, Naragh Branch, Islamic Azad University, Naragh, Iran

[3] Assistant Professor, Department of Computer, Naragh Branch, Islamic Azad University, Naragh, Iran

Article Info

Original Article

Received:
12-11-2022
Accepted:
24-12-2022

Keywords:
Anti-forensics
Data
Digital forensics
Data protection
Obtaining evidence

***Corresponding author**
e-mail: sepehrio@gmail.com

Abstract

In obtaining digital evidence, one has to take many different steps. Regarding this, criminal systems still have not agreed upon a unique standard, particularly in the case of digital evidences. Digital forensics, as a science concerning the processes of obtaining evidence, proposes anti-forensic methods that, if they are paid attention to, countries can make their laws more technical in terms of content. Unfortunately, digital forensics does not have a favourable situation in terms of theory and practice. In this respect, the weakness of Acts and instruments such as the Iranian criminal procedure Act and the regulations regarding collecting electronic evidence is apparent. This essay has examined the challenges in digital forensics with a descriptive approach and seeks to approximate them by applying the rules of Iran and English criminal systems.

How to Cite:
Khosravizad, A., Sepehri, R., & Bababee, H. (2022). Digital Forensics in Iran and English Criminal Systems. *Modern Technologies Law*, *3*(6), 155-172.

Published by University of Science and Culture https://www.usc.ac.ir
Online ISSN: 2783-3836

حقوق فناوری‌های نوین

http://doi.org/10.22133/MTLJ.2022.369536.1142

دیجیتال فارنزیک در نظام کیفری ایران و انگلستان

افشار خسروی‌زاد[۱]، روح‌الله سپهری[۲]*، حمیده بابایی[۳]

[۱] دانشجوی دکتری، گروه حقوق کیفری و جرم‌شناسی، واحد نراق، دانشگاه آزاد اسلامی، نراق، ایران

[۲] استادیار گروه حقوق، واحد نراق، دانشگاه آزاد اسلامی، نراق، ایران

[۳] استادیار گروه کامپیوتر، واحد نراق، دانشگاه آزاد اسلامی، نراق، ایران

اطلاعات مقاله

مقالهٔ پژوهشی

تاریخ دریافت:
۱۴۰۱/۸/۲۱

تاریخ پذیرش:
۱۴۰۱/۱۱/ ۳

واژگان کلیدی:
آنتی‌فارنزیک
پردازش داده
تحصیل دلیل دیجیتال
دیجیتال فارنزیک
نظام ادلهٔ کیفری

***نویسندهٔ مسئول**
رایانامه: sepehrio@gmail.com

نحوهٔ استناددهی:
خسروی‌زاد، افشار، سپهری، روح‌الله و بابایی، حمیده (۱۴۰۱). دیجیتال فارنزیک در نظام کیفری ایران و انگلستان. حقوق فناوری‌های نوین، ۳(۶)، ۱۷۲-۱۵۵.

ناشر: دانشگاه علم و فرهنگ https://www.usc.ac.ir
شاپای الکترونیکی: ۲۷۸۳-۳۸۳۶

چکیده

امروزه تحصیل دلیل دیجیتال جایگاهی ویژه یافته است؛ زیرا مجرم سایبری همواره در کمین قرار دارد تا ادلهٔ مرتبط با جرم به دست متخصصان فارنزیک نرسد. ازاین‌رو، قواعد علم دیجیتال فارنزیک برای جلوگیری از اقدامات مجرمان سایبری و حفظ تمامیت و محرمانگی داده‌ها طراحی شده است تا نظام‌های کیفری، با پذیرش آن، قواعد کارآمدتری را برای جوامع اعتبار و عرضه کنند. در این تحقیق، با بررسی تطبیقی‌تقریبی دو نظام کیفری انگلستان و ایران در سه بخش (پیش از تحصیل دلیل، حین تحصیل دلیل و پس از تحصیل دلیل)، نظام کیفری‌فارنزیک ایران بسیار ضعیف و ناتوان از تقلید بازشناسایی شد. یکی از این دلایل عدم پیش‌بینی اقدامات آنتی‌فارنزیک در قوانین ایران و به‌ویژه در آیین‌نامهٔ جمع‌آوری و استنادپذیری ادلهٔ الکترونیکی ۱۳۹۳ است. در نهایت، پیشنهادهایی دربارهٔ زمان حذف پوشهٔ ریکاوری، مأمور توقیف و تفتیش داده، و مکان آنالیز داده‌ها ارائه شده است.

مقدمه

محققان در حوزهٔ جرائم الکترونیکی کم قلم نزده‌اند؛ پیشنهادهایی نیز ارائه کرده‌اند که در مرتبه و زمان خود قابل تحسین بوده است. اما دو اشکال در این آثار دیده می‌شود؛ اول آن‌که برخی از نویسندگان جرم رایانه‌ای را موضوع بحث قرار داده‌اند و با آن به مباحثی همچون تحصیل ادله و استنادپذیری ادلهٔ الکترونیکی پرداخته‌اند (بابایی، ۱۴۰۰، ص ۲۹۷-۳۰۴). دوم آن‌که از مهم‌ترین منابع قانونی در این زمینه مانند قوانین حمایت از داده استفاده نشده است (السان، ۱۳۹۹، ص ۲۶۶-۲۶۷). حقوق انگلیس از دو جهت اهمیت بسزایی در مطالعهٔ تطبیقی جستار در دست دارد؛ اولاً، با وجود پذیرش مقررات حفاظت از داده‌های ۲۰۱۸[1]، مقررات ویژه‌ای دربارهٔ حمایت از داده‌ها وضع کرده است.[2] از مهم‌ترین آن‌ها می‌شود به قانون حمایت از دادهٔ مصوب ۲۰۱۸[3] اشاره کرد. ثانیاً نظام دلایل قانونی این کشور دلایل دیجیتال فارنزیک را به‌منزلهٔ دلیلی مستقل پذیرفته و بدان بها داده است که نقطهٔ مقابل حقوق ایران به‌شمار می‌رود.

جنبه‌های متعددی برای دلیل دیجیتال برشمرده‌اند که هریک را می‌شود موضوع بررسی قرار داد. برخی از نویسندگان همچون اریک هولدر[4] دلایل دیجیتال را از سه منظر حائز واکاوی می‌دانند:[5] فنی، حقوقی و مرتبط با منابع (Singh, 2021, p. 26). فرض کنید موبایل الف محتوای مجرمانه دارد. با قرارگرفتن در هوای بسیار گرم اطلاعات پاک می‌شود. ازاین‌رو بازخوانی اطلاعات برای متخصصان پرسش‌ها و مشکلاتی را به همراه آورده است. اگر همین مثال را چنین تغییر دهیم، موبایل الف به‌سبب نقض فنی، مسائل زیست‌محیطی و... خودکار و ناخواسته با شماره‌ای تماس می‌گیرد که دارندهٔ شماره مظنون اصلی جرم سرکردگی گروه تروریستی است، این موضوع نیز حقوقی-تخصصی به‌نظر می‌رسد. جنبهٔ سوم نیز تحت عنوان منابع[6] قابل‌احصا است. بدین تعبیر که حجم داده‌ها، مدت زمان لازم برای دست‌یابی به داده‌ها و حتی منابع انسانی لازم در صورت افزایش جرائم سایبری پرسش‌هایی هستند که این رشته باید به آن‌ها پاسخ دهد. پرسش اصلی این جستار آن است که تفاوت‌های بنیادین دیجیتال فارنزیک در نظام کیفری ایران و انگلستان چیست. با توجه به موضوع، سعی شده است تا راهکارهایی ارائه شود که این دو نظام تا حد امکان به یک‌دیگر نزدیک شوند و خلأهای نظام کیفری ایران ترمیم شود.

اثر پیش‌رو در سه بخش تنظیم شده است: بخش اول به تعاریف و مبانی می‌پردازد. در بخش دوم، دیجیتال فارنزیک و آنتی‌فارنزیک و فرایندهای آن مورد بررسی قرار می‌گیرد. درنهایت، موضع دو نظام کیفری انگلستان و ایران در مواجهه با دیجیتال فارنزیک بیان شده است.

۱. تعاریف و مبانی

۱-۱. تعریف دلیل

اهل لغت دلیل را از ریشهٔ دَلَل و به معنای راهنما و اماره می‌دانند (احمد بن فارس، ۱۴۰۴ه.ق، ص۲۵۹). بنابراین، هرچیزی که دیگری را راهنمایی کند دلیل گویند. مفهوم دلیل در دیدگاه حقوقی نیز از معنای لغوی آن فاصله نگرفته است.

در حقوق کیفری ایران دو تعریف بسیار رایج است: الف) ۱-. دلیل به معنای عام: استناد به وسیله‌ای برای اثبات امری. ۲.دلیل به معنای خاص: شیوه‌های به‌کارگرفته‌شده برای اثبات واقعیت‌داشتن امر یا رخدادی (گلدوزیان، ۱۳۸۲، ص۱۶).

ب) دلیل شامل اثبات وجود یک عمل، انتساب آن به یک شخص و معمولاً قصد وی در ارتکاب عمل مذکور است (میرمحمدصادقی، ۱۳۸۳، ص۳۸۵).

---

1. General Data Protection Regulation

۲. شایان ذکر است که همچنان انگلستان تابع مقررات جی.دی.پی آر است و به‌موجب قانون بریگزیت از مقررات مذکور خارج نشد.

3. Data Protection Act -United Kingdom-2018 (DPA)
4. Eric Holder
5. Deputy Attorney General of the United States Subcommittee on Criminal Oversight for the Senate
6. Resource

تعریف دلیل در حقوق انگلیس نیز یکسان نیست و بر سر آن اختلاف وجود دارد. دو تعریف رایج از قرار زیر است:

الف) اطلاعاتی است که به دادگاه و قاضی یا هیئت منصفه داده می‌شود تا ایشان را در راستای این استنتاج که جرم رخ داده یا خیر مساعدت کند

ب) دلیل سعی در اثبات صدق یا احتمال صدق واقعیتی (یا امری) را دارد اما به هر حال نحوهٔ ارائهٔ دلیل در مقابل دادگاه و هیئت منصفه است.[۱]

تعریف دیگری از دلیل نیز وجود دارد: هرچیزی (از قبیل، شهادت، سند یا اشیای محسوس) که در اثبات یا عدم‌اثبات واقعهٔ ادعایی کارسازی کند (Hails, 2009, p. 2).

۲-۱. انواع دلیل کیفری در حقوق انگلیس

درحقوق انگلیس حدود هفت دلیل در امر کیفری شمرده شده است. دلیل مستقیم یا ادراکی،[۲] دلیل مرتبط با اوضاع و اوحوال،[۳] دلیل اولیه،[٤] دلیل ثانویه،[٥] دلایل فارنزیک،[٦] دلیل مبتنی بر نظر متخصص،[۷] دلیل ظاهر[۸] (Singh, 2022, p. 6).[۹] دلیل مستقیم دلیلی است که خود شخص بدون واسطه آن را دیده، لمس کرده یا شنیده است (Del Carmen & Hemmens, 2017, p. 54). برای مثال، اگر شاهد از روی شایعه یا قول شخص دیگری در برابر قضات اقدام به شهادت کند، دلیل ارائه‌شده دیگر مستقیم یا ادراکی تلقی نمی‌شود. به بیان دیگر، در لحظهٔ تحمل واقعه باید شخص متحمل واقعهٔ مذکور را با حواس خود بدون دخالت شخص دیگر تحمل کند. دو معنا برای دلیل مستقیم وجود دارد: ۱. دلیل مستقیم در برابر دلیل مرتبط با اوضاع و احوال؛ ۲. تعریف مضیق. دلیل مستقیم به معنای شاهدی که بیان می‌کند در واقع امری را درخصوص موضوعی دیده یا شنیده یا حس کرده است (Anderson et al., 2005, p. 382). دلیل مرتبط با اوضاع و احوال، برخلاف دلیل مستقیم، نیازمند استنتاج بعدی دادگاه است. بدین توضیح که دادگاه به صرف توضیح، بیان یا رؤیت آن نمی‌تواند رأی صادر کند. برای مثال، الف می‌گوید ب در هنگامی که قرارداد را امضا می‌کرد آواز می‌خواند که ممکن است دلیلی بر مست‌بودن ب باشد (Singh, 2022, p. 6). برخی اوقات راه استنتاج و بررسی بعدی دادگاه آسان است، مثلاً تست الکل در مثال مذکور. در مقابل، گاهی این استنتاج سخت است مانند مضی زمان بسیار از زمان تحمل تا شهادت در دادگاه، که تست الکل نیز نافرجام می‌ماند. ازاین‌رو، در نظر عموم مردم، دلیل مستقیم از دلیل مبتنی بر اوضاع و احوال قوی تر است. اما این گزاره همواره مطابق واقع نیست. برای مثال، دفاع از تست دی ان ای که نوعی دلیل مبتنی بر اوضاع و احوال است بسیار سخت و دشوار است، درحالی‌که برخی از مطالعات نشان می‌دهد که شهادت عینی به‌راحتی قابلیت دفاع دارد و قابلیت استناد ندارد! (Anderson et al., 2005, p. 383) از سوی دیگر، می‌توان گفت بهترین نوع دلیل دلیل اولیه است. این نوع از دلیل در طبقه‌بندی نظام ادلهٔ حقوق کامن لا شامل اصول اسناد یا به بیان بهتر خود موضوع جرم است. برای مثال، چاقوی آغشته به خون نزد قاضی آورده می‌شود یا سندی که رفتار مادی جعل به روی آن رخ داده است تماماً از دلایل اولیه به‌شمار می‌روند (Singh, 2022, p. 8). کپی‌های سند نیز، در صورتی که اصل سند در پرونده باشد یا قابل دسترس باشد، دلیل اولیه احصا شده است (Hails, 2009, p. 182).

1. See: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/919630/evidence-in-criminal-investigations-v5.0.pdf, Last visited on: 11/11/2022
2. Direct or percipient evidence
3. Circumstantial evidence
4. Primary evidence
5. Secondary evidence
6. Forensic evidence
7. Expert evidence
8. Presumptive or prima facie evidence
9. See also: https://www.draycottbrowne.co.uk/investigations/types-evidence Last visited on: 11/7/2022

در مقابل هر دلیلی که بتواند جای خالی دلیل اصل را پر کند، دلیل ثانوی نامیده می‌شود. برای مثال، شهادت بر این‌که در سند تنظیمی چه مفادی مقرر شده بود (Parol evidence)، پیش‌نویس قرارداد یا نسخهٔ کپی قرارداد (Hails, 2009, p. 185). البته شایان توجه است که درخصوص نسخهٔ کپی چند استثنا وارد است و در صورت وجود هریک ازاین استثنائات دیگر دلیل جزء دلایل اولیه به‌شمار می‌رود، مانند اصل در تصرف خوانده باشد، اصل غیرقابل دسترس باشد، اصل مفقود یا تخریب شده باشد و... .[1]

گسترهٔ دلیل دیجیتال فارنزیک از دلایل پیشین متفاوت است و به دلایل به‌دست‌آمده در فضای سایبر اطلاق می‌شود. برای مثال، فایل دیجیتالی که حذف شده توسط متخصص امکان بازیابی دارد و از این طریق تحصیل دلیل میسر می‌شود. مثال‌های سنتی این نوع از دلیل فرایندهای پزشکی قانونی در مواجهه با قربانی یا متهم است. برای مثال، ازمایش الکل، ادرار، یا دی ان ای. اما، با توجه به پیشرفت فناوری، مهارت‌های فارنزیک فقط به پزشکی محدود نشده و به فضای دیجیتال نیز سرایت کرده است. برای نمونه به جدول ۱ توجه کنید:

جدول ۱: نحوهٔ ریکاوری پوشهٔ تخریب‌شده (اقتباس از مور (2005, p. 67))

عنوان فایل تخریب (دیلیت) شده	عنوان فایل اصلی (قبل از تخریب)
E5esume.doc	Resume.doc
E5udget.xls	Budget.xls

چنان‌که در جدول ۱ مشاهده می‌شود، عنوان فایل تخریب‌شده نمایهٔ هگزادیسیمال[2] فایل اصلی است.

دلیل دیگری که در حقوق کیفری انگلستان اعتبار دارد دلیل متخصص است.گاهی اوقات دادگاه، بیش از آن‌که به دلیل عینی نیاز داشته باشد، به نظر متخصص نیاز دارد. برای مثال، فرض کنید تمامی مواد خام و دلایل نزد دادگاه موجود است اما دادگاه دانش و مهارت کافی در موضوع را ندارد. این نوع دلیل بسیار شبیه قرار کارشناسی در حقوق ایران است، اما با آن فرق دارد. اصولاً اسباب حکمی از جانب طرفین و شهود یا مطلع نزد دادگاه پذیرفته نمی‌شود و صرفاً اسباب موضوع و شواهد پذیرفته می‌شود. اما، درخصوص دلیل متخصص، دادگاه ممکن است آن را قبول کند و در رأی خود تأثیر دهد. برای مثال، دعوایی که در سال ۱۷۸۲ اقامه شد[3] نمونهٔ بارز و ازجمله آرای مؤسس در زمینهٔ پذیرش دلیل متخصص است.[4] به‌هرحال، دلایل در حقوق کیفری انگلستان به همین مقدار بسنده نشده است و وقتی دو قاعده یا فرض قانونی با یکدیگر تعارض می‌کنند، دادگاه مخیر است آن‌که قوی‌تر می‌داند اعمال کند (دلیل ظاهر).

در ایران، تا انقلاب سال ۱۳۵۷ هیچ اثری از علم قاضی به‌منزلهٔ دلیل یا نتیجهٔ آن در قوانین مصوب نبود. پس از پیروزی در انقلاب، در چند مورد علم قاضی مطرح شد (مدنی، ۱۳۷۸، ص۳۷۶). برای نمونه، در قانون مجازات اسلامی سال ۱۳۷۰ چنین مقرر شده بود: «حاکم شرع می‌تواند در حق‌الله و حق‌الناس به علم خود عمل کند و حد الهی را جاری نماید و لازم است مستند علم را ذکر کند، اجرای‌حد در حق‌الله متوقف به درخواست کسی نیست ولی در حق‌الناس اجراء حد موقوف به درخواست صاحب حق می‌باشد.» برخی از محققان، در همین خصوص، علم قاضی تحقیق را نیز برای قاضی دادگاه به عنوان اماره احتساب کرده‌اند (یثربی، ۱۳۸۵، ص۷۰). در مادهٔ ۱۲۰ از حیث تأکید مجددا مقرر می‌شود: «حاکم شرع می‌تواند طبق علم خود که از طرق متعارف حاصل حکم شود کند.» به نظر نیازی به قید از طرق متعارف نیز نیست، چرا که علم با تعریفی که فقها نموده‌اند از طرق متعارف به‌دست می‌آید. تنها دلیل ذکر طرق متعارف آن است، که هیچ کس نباید قاضی پروندهٔ خود باشد[5].البته خواب، رؤیا و وهم نیز موضوعاً از مادهٔ مذکور به‌سبب واژهٔ علم خارج است. به‌هرحال، رویکرد نوین

1. Federal Rules of Evidence, Rule 1004

۲. هگزادیسیمال (hexadecimal) سامانهٔ عددنویسی است که بر مبنای عدد ۱۶ است. این سامانه برخی از اعداد را به شکل خود نشان می‌دهد (اعداد ۰تا۹) و بعضی دیگر را (۱۰-۱۵) به ترتیب با حروف (A-F) نمایش می‌دهد. https://www.sciencedirect.com/topics/engineering/hexadecimal

3. Folkes v Chadd (1782)99 E.R. 589

٤. برای مطالعهٔ بیشتر شرایط پذیرش دلیل متخصص ر.ک: مادهٔ ۱۹ مقررات دادرسی کیفری انگلستان و ویلز (The Criminal Procedure Rules 2020)

٥. Nemo iudex in causa sua؛ این قاعدهٔ رومی به این معناست که هیچ‌کس نمی‌تواند قاضی پروندهٔ خویش باشد (آقایی، ۱۳۷۸، ص ۸۴۸).

قانونگذار سال ۱۳۹۲ نیز به تمامی اختلافات پایان نداده است و هنوز بر سر علم حصولی یا شخصی، نوع سیستم (دلایل معنوی یا قانونی) از حیث تعارض علم قاضی با سایر ادله و... اختلاف است (حیدری، ۱۳۹۳). با توجه به موضوع پژوهش حاضر، فرض را بر تمایل اکثر حقوق‌دانان و فقها (هاشمی شاهرودی، ۱۳۷۸، ص ۷۱و ۷۲) و ظاهر مادهٔ ۲۱۱ قانون مجازات ۱۳۹۲ می‌گذاریم و بحث را ادامه می‌دهیم.

۲. تحصیل دلیل دیجیتال: کلیات فارنزیک، آنتی‌فارنزیک، روش‌شناسی

همان‌طور که در مقدمه بیان شد، نفس تحصیل دلیل[۱] از جهات افتراق علم تحصیل دلیل کیفری با تحصیل دلیل دیجیتال نیست، بلکه ویژگی‌هایی به جدایی این دو منجر شده است. در این بخش به شاخصه‌هایی می‌پردازیم که هردو نظام کیفری ایران و انگلیس توان پذیرش آن را دارند.

۲-۱. علم دیجیتال فارنزیک

به دنبال پیشرفت‌هایی که در ارتکاب جرائم به‌وجود آمده است، تحصیل دلیل نیز مواجه با تغییراتی بوده است. در این راستا، ابتدا برای جرم‌کاوی کامپیوتر فارنزیک و سپس با پیشرفت فناوریْ دیجیتال فارنزیک در نتیجهٔ ظهور انواع جرائم سایبری توسعه یافت. علم دیجیتال فارنزیک بدون نگاه به منشأ یا ملیت راهنمایی را برای نظام‌های قضایی گوناگون ارائه می‌دهد تا بتوانند ادلهٔ دیجیتال را تحصیل کنند (ابوالمعالی الحسینی، ۱۳۹۵، ص ۲۶۱). ناگفته نماند که مجرمان واقعی نیز با احساس خطر کردن دست به اعمالی می‌زنند که به اصطلاح آنتی‌فارنزیک نامیده می‌شود که به توضیح آن خواهیم پرداخت.

۲-۲. تعریف دیجیتال فارنزیک

در تعریفی ساده، به استفاده از دانش برای جمع‌آوری، پردازش و ارائهٔ ادله در دادگاه فارنزیک می‌گویند. این فرایند ممکن است شامل اطلاعات یا داده‌هایی شود که داخل سخت‌افزار یا نرم‌افزار رایانه، موبایل، دستگاه جی پی اس، ماشین‌های دیجیتال و هر وسیلهٔ دیجیتال دیگر قراردارد.[۲] فارنزیک در لغت به معنای ارائه به دادگاه است. اما فارنزیک در شروع فرایند خود با بازیابی[۳] و آنالیز[٤] ادلهٔ پنهان[٥] سروکار دارد. ادلهٔ پنهان قالب‌های متنوعی دارند: از اثر انگشت روی پنجره گرفته تا لکهٔ خونی که دی ان ای متهم را مشخص می‌کند و همچنین فایل‌هایی که روی سخت‌افزار[٦] وجود دارد (US-CERT, 2008, p. 1). تعریف آکادمی علوم فارنزیک آمریکا (AAFS)[۷] اما چنین است: فارنزیک از واژهٔ لاتین Forensis به معنای عمومی، بحث عمومی، انجمن، استدلالی، بلاغی، مربوط به بحث یا مناقشه مشتق شده است. در تعریفی مرتبط و مدرن می‌توان گفت که علم فارنزیک عبارت است از هرچیزی که که مرتبط با دادگاه باشد یا برای آن مناسب باشد. هر دانشی که برای اهداف قانونی استفاده شود، دانش فارنزیک نام دارد. علوم فارنزیک در سراسر جهان برای حل‌و فصل اختلافات مدنی و اجرای عدالت کیفری، مقررات دولتی وحفظ سلامت عمومی به‌کار گرفته می‌شوند.[۸]

---

۱. امروزه، دو مکتب تحصیل دلیل سنتی و نوین شکل گرفته است. برای مطالعهٔ شاخصه‌های تحصیل دلیل سنتی می‌توان به کتب سنتی که عهده‌دار تدوین قواعد برای جرائم فیزیکی شده‌اند مراجعه کرد.

2. https://www.techopedia.com/definition/27805/digital-forensics written by Margaret Rouse, 2022 (Last visited on 12/3/2022)
3. Recovery
4. Analysis
5. Latent evidence
6. Hard drive
7. American Academy of Forensic Science (AAFS)
8. https://www.aafs.org/careers-forensic-science/what-forensic-science [American Academy of Forensic Science (AAFS)] (Last visited on 11/3/2022)

۲-۳. تاریخچهٔ دیجیتال فارنزیک

تاریخچهٔ دیجیتال فارنزیک به چهل سال پیش بازمی‌گردد. در اواخر دههٔ ۱۹۷۰، طی تقاضاهایی که به دلیل افزایش جرائم کامپیوتری به‌وجود آمده بود، بازرسان شروع به تفتیش از کامپیوترها به‌عنوان منبع دلیل کردند.

در سال ۱۹۸۴، گروه تحقیقات رایانه‌ای همکاری خود را با پلیس فدرال آمریکا (FBI)[1] آغاز کرد و پلیس فدرال را در توقیف و تفتیش و بازرسی فارنزیک رایانه‌ها و جمع‌آوری ادله حمایت کرد. در سال ۱۹۹۰، مصرف اینترنت و فناوری چشمگیر شد که به دنبال آن اینترنت صحنهٔ وقوع جرائم قرار گرفت. به عبارت دیگر، رشد فزایندهٔ مصرف اینترنت سبب تسهیل حملات اینترنتی نیز شد. در همین بحبوحه، آکادمی بین‌المللی اجرای قوانین در سال ۱۹۹۵ میلادی با هدف کاهش جرائم، مبارزه با تروریسم و اشتراک‌گذاری فناوری‌های نوین شکل گرفت. در سال ۱۹۹۷ نیز کارگروه علمی دلایل دیجیتال (SWGDE)[2] برای تنظیم اصول و قواعد علم فارنزیک تشکیل شد. جرائم سایبری در سال ۲۰۰۰ بسیار گسترش یافت و ادلهٔ دیجیتال دستگاه‌های موبایل را نیز دربرگرفت. سال ۲۰۰۱ کارگروه تحقیقات دیجیتال فارنزیک (DFRWS)[3] کار خود را که جمع‌آوری محققان، مؤسسات، ابزارها، استادان، دستگاه‌های اجرایی و نظامی برای به‌چالش‌انداختن علم دیجیتال فارنزیک بود شروع کرد. در این دوران کارهای شگرفی در این حوزه از سوی محققان در سراسر دنیا انجام شد (Prasanthi, 2016, p.266). واژگانی چون دیجیتال فارنزیک، کامپیوتر فارنزیک، کشف مدارک دیجیتال[4] یا الکترونیک، با آن‌که معانی نسبتاً یک سانی دارند (ابوالمعالی الحسینی، ۱۳۹۵، ص ۲۶۱)، اما از حیث مفهومی رابطهٔ تباین و از حیث مصداقی رابطهٔ عموم خصوص مطلق یا من وجه دارند. بدین توضیح که دیجیتال فارنزیک چند نوع دارد: کامپیوتر فارنزیک، موبایل فارنزیک،[5] نتورک فارنزیک (فارنزیک شبکهٔ اتصال)،[6] فارنزیک پایگاه داده.[7] از همهٔ این موارد تحت عنوان دیجیتال فارنزیک یاد می‌شود. پس می‌توان گفت فرایند دیجیتال فارنزیک، همان‌طور که از نام دیجیتال پیداست، جامع‌تر از انواع فارنزیک‌های مرتبط با کالاها و ابزارهای دیجیتال است.[8]

۲-۴. آنتی‌فارنزیک

تعریف منحصربه‌فردی از آنتی‌فارنزیک ارائه نشده است. ازاین‌رو برخی چنین بیان داشته‌اند: «جای تعجب نیست که تعریف جامع و واحدی از این موضوع وجود ندارد، زیرا مفهومی نوین است. برخی از تعاریف صرفاً به بعضی از شاخصه‌های این مفهوم نظر انداخته‌اند و برخی دیگر جامع‌تر موضوع را بررسی کردند. برخی مانند فوستر و لیو نفوذ و ابزارهای نفوذکننده را داخل تعریف می‌کنند و بعضی دیگر مانند شیرانی فقط نفوذ سیستمی را مشمول تعریف می‌داند.» (Harris, 2006, p. 45)

برخی دیگر اما تعریفی ساده از این واژه ارائه داده‌اند که به نظر قابل انتقاد است: «آنتی‌فارنزیک فرایند متقابل فارنزیک است. در واقع به اقداماتی که برای محو و فرارکردن از تحقیقات فارنزیک به‌عمل می‌آید فرایند آنتی‌فارنزیک می‌گویند. هدف اصلی آنتی‌فارنزیک آن است که ادلهٔ جرم به دست بازرسان و مأموران دادگستری نرسد.» (Jain & Chhabra, 2014, p. 412)

---

1. Federal Bureau of Investigation
2. Scientific Working Group on Digital Evidence
3. Digital Forensic Research Workshop
4. Electronic Evidence Discovery
5. Mobile Device Forensics
6. Network Forensics
7. Database Forensics

۸. وفق مادهٔ ۱۹ دستورالعمل حقوق مصرف‌کنندگان (Directive 2011/83/EU of 25.11.2011 on consumer rights (CRD))، محتوای دیجیتالی شامل رایانه، برنامه‌های رایانه‌ای، موسیقی، بازی‌های رایانه‌ای، ویدئوها و... می‌شود. به‌طور کلی می‌توان گفت هرآنچه دارای دادهٔ رایانه‌ای است وسیله‌ای دیجیتالی است. برای مطالعهٔ بیشتر ر.ک: جعفرزاده و عاکفی قاضیانی، ۱۴۰۱. داده‌رایانه نیز مجموعه‌ای از نمادها،حروف، اعداد و علائم و در مقابل برای رایانه شامل رمزهای صفر و یک است که وقایع و حقایق را نشان می‌دهد. داده‌ها برای انسان از طریق حواس پنج‌گانه و برای رایانه از طریق لوازم مخصوص مانند صفحه کلید، موس و غیره تحصیل می‌شود. برای استفاده از داده (توسط انسان) باید آن‌ها را پردازش کرد (عبدی پور فرد، وصالی ناصح، ۱۳۹۶، ص ۹۰)

با توجه به آنچه تا کنون بیان شد، به‌نظر می‌آید که تعریف لغوی از تعریف مصطلح (حقوقی) فاصله گرفته است و همان‌طور که فرهنگ لغت مریام وبستر (Merriam-Webster, 2003) در تعریف پیشوند (anti) بیان می‌کند: در مقابل یا خلاف با، نمی‌توان آنتی‌فارنزیک را تفسیر و تعبیر حقوقی کرد. درحالی‌که تفسیر پیشین (تفسیر جین) کاملاً لغوی است.

برای مثال، آیا خود مأموران و قوای دولتی که هیچ نقشی در ارتکاب جرم ندارند نمی‌توانند عملیات آنتی‌فارنزیک را انجام دهند؟ ازاین‌رو واژه نیاز به بازتعریف دارد.

از آن رو که عملیات فارنزیک در جهت پیداکردن ادلهٔ متناسب با جرم است، می‌شود به تعاریف جرم‌محور آنتی‌فارنزیک نیز دقت کرد. پرون و لگاری[1] آنتی‌فارنزیک را اقداماتی برای محدودسازی شناسایی، جمع‌آوری، طبقه‌بندی و اعتبارسنجی داده‌های الکترونیکی می‌دانند (Harris, 2006, p.45). به نظر هریس، این تعریف نیز کامل نیست چون ادله را دربر نگرفته و موضوعیت را به داده‌های الکترونیکی داده است. اما تعریف گروگ[2] چنین است: اقدام و تلاش برای محدودسازی ادلهٔ فارنزیک.[3] به نظر هریس این تعریف با آن‌که ادله را دربر گرفته است اما به فرایند فارنزیک اشاره نکرده است! به نظر هریس، اگر دو تعریف گروگ و پرون و لگاری را ترکیب کنیم، تعبیری دقیق و جامع از آنتی‌فارنزیک به‌دست می‌آید.

نهایتاً تعریف هریس از آنتی‌فارنزیک عبارت است از: هر نوع اقدامی که قابل استفاده بودن یا در دسترس بودن ادله را در فرایند فارنزیک به مخاطره بیندازد آنتی‌فارنزیک نام دارد.

به‌نظر می‌رسد تعریف هریس و مداقه‌ای که نموده است جامع نباشد. اولاً آیا «زمان‌خریدن» (در اصطلاح عرفی) دخیل در مفهوم آنتی‌فارنزیک است؟ برای مثال، متهم انگشتان خود را به دیوار می‌کشد تا کمی دیرتر شناسایی شود. این عمل معادل آنتی‌فارنزیک در فضای دیجیتال است که در واقع در فضای مادی رخ می‌دهد. حال در فضای دیجیتال متهم رمز صفحهٔ گوشی خود را بعد از مدتی تغییر می‌دهد تا عملیات فارنزیک به طول انجامد؛ آیا این عملیات آنتی‌فارنزیک به‌شمار می‌رود. به عبارت بهتر، ادله به مخاطره نمی‌افتند اما زمان وصول به آن‌ها تغییر می‌کند. ثانیاً، با توجه به آن‌که آنتی‌فارنزیک چه ضمانت اجرایی در قوانین ملی دارد، باید تعاریف تفاوت کند. بنابراین نمی‌توان معتقد بود که عملیات آنتی‌فارنزیک، وقتی توسط متخصص فارنزیک پلیس انجام می‌شود تا گپ‌های موجود در سیستم اطلاعاتی را دریافت کند، مرتکب رفتار مادی جرم آنتی‌فارنزیک شده است. آنتی‌فارنزیک طبق نظر غالب انواعی دارد. به عبارت دیگر، «به‌مخاطره‌انداختن» فارنزیک انواعی دارد.

۲-۵. انواع آنتی‌فارنزیک

نظر غالب آن است که اقدامات آنتی‌فارنزیک در چهار نوع قابلیت تقسیم دارد:

۱. مخفی‌کردن داده‌ها
۲. پاک‌کردن داده‌ها
۳. مبهم‌کردن مسیر و دنباله‌ها
۴. حملات علیه فرایند فارنزیک و ابزارهای آن (Shanmugam, 2011, p. 29)

1. Peron and Legary
2. Grugq
3. Grugq The art of defiling: defeating forensic analysis Blackhat briefings 2005 (2005) http://www.blackhat.com/presentations/bh-usa-05/bh-us-05-grugq.pdf (Harris, 2006)

۲-۵-۱. مخفی‌کردن داده‌ها[1]

استگانوگرافی،[2] مورس[3] و رمزنگاری پوچ[4] از شیوه‌های رایج مخفی‌کردن ادله‌اند. استگانوگرافی یا همان پنهان‌نگاری سابقهٔ پانصدساله (از سال ۱۴۹۹ میلادی) دارد. کارکرد پنهان‌نگاری به‌گونه‌ای است که داده را شکل و ماهیتی دیگر می‌بخشد. داده‌های پنهان‌نگاری‌شده در قالب فایل‌های صوتی، تصویری (اعم از ویدئو یا عکس)، فایل خام و پروتکل قابل انتقال‌اند (Shanmugam, 2011, p. 30)؛ حتی قابل جاسازی در فضای عمومی‌اند. مثلاً یک عبارت پنهان‌نگاری را درنظر بگیرید که معنای آن می‌شود: بمب‌گذاری رأس ساعت Y در خیابان X. متخصصان آنتی‌فارنزیک می‌توانند رمز این عبارت را به‌صورت رنگ سفید در پیش‌زمینهٔ سایتی عمومی که رنگ سفید دارد قرار دهند و افراد تیم بمب‌گذار با دسترسی به سایت عمومی عبارت مذکور را کپی و نهایتاً رمزگشایی کنند و از زمان و مکان مطلع شوند.

رمزنگاری پوچ هم تا حدی شبیه به پنهان‌نگاری است اما هیچ معنایی ندارد. برای مثال، این سطر شاید رمزی پوچ تلقی شود: 1436589047b79fkl. گروهک‌های ماهر، به‌صورت رمزنگاری، رمزها را برای یک‌دیگر بازگشایی می‌کنند. مثلاً دفترچهٔ رمزگشا دارند و طبق آن هرروز رمزهایی میانشان رد و بدل می‌شود؛ به هگزادیسیمال در علم رایانه و ابجد هوز در علوم غریبه بسیار شبیه است.

۲-۵-۲. پاک‌کردن داده‌ها[5]

برخلاف پنهان‌کردن دادها، در پاک‌کردن داده‌ها به‌کلی محو می‌شوند. پاک‌کردن داده‌ها ممکن است از طریق پاک‌کردن کل سیستم‌های مرتبط با فایل صورت گیرد (چه فیزیکی و چه مجازی) یا با حذف فایل یا داده‌ای به‌خصوص انجام شود. این کار روش‌های گوناگونی دارد که خواننده قطعاً با برخی از روش‌های آن آشناست؛ اما باید توجه داشت که روشی مانند شیفت+دیلیت (Shift+del) قابل ردیابی و بازیابی است؛ زیرا فایل حذف‌شده به سخت‌افزار منتقل می‌شود. با وجود این، ابزارهایی برای حذف نهایی فایل از سخت‌افزار وجود دارد:[6] BC Eraser،WIPE و PGP Wipe. ولی به گفتهٔ جین فارنزیک را ازبین نمی‌برد بلکه اقدامات فارنزیکی را سخت می‌کند (به عبارت دیگر ردیابی فایل یا بازگشت آن حتی در صورت حذف از سخت‌افزار نیز امکان دارد) (Jain & Chhabra, 2014, p. 413).

۲-۵-۳. مبهم‌کردن مسیر و دنباله‌ها[7]

این روش نوعی اقدام برای منحرف‌کردن تحقیقات فارنزیک است. روش و مبنای انجام آن مبتنی بر همان اصول استگانوگرافی یا تزریق داده‌های نادرست است. در این روش، مجرمان سایبری با به‌کارگیری پروتکل‌های شبکهٔ همتابه‌همتا (P2P)[8] دست به اقدامات خود می‌زنند. در نتیجهٔ این استفاده، رد پای ایشان و اثر انگشت بیومتریک سایبری آن‌ها از انظار پنهان می‌ماند (Yaacoub et al., 2021, p. 26). دو روش رایج در مبهم‌سازی مسیر فارنزیک «تغییردادن»[9] و «تغییر شکل/ قالب دادن»[10] است (Shanmugam, 2011, p.32).[11] در تغییردادن، مجرم

---

1. Data hiding
2 .steganography
3. Morse code messages
4. Null ciphers
5. Artifact wiping

٦. برای دیدن آمار ابزارهای موجود برای هریک از شیوه‌های آنتی‌فارنزیک به مقاله زیر رجوع کنید:

Conlan, K., Baggili, I., & Breitinger, F. (2016). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. Digital Investigation, 18, S66-S75.

طبق این آمار، بیشترین ابزار آنتی‌فارنزیک برای همین بند موردبحث (پاک‌کردن داده) تولید شده است و در بازار موجود است.

7. Trail obfuscation

۸. شبکهٔ همتا به همتا یا نظیر به نظیر (Peer to peer) به تعبیر ساده نوعی از شبکه‌های رایانه‌ای است. در این نوع شبکه دیگر سرویس‌دهنده و متقاضی سرویس وجود ندارد، بلکه هردو رایانه در یک سطح قرار دارند و هر رایانه می‌تواند اطلاعات رایانهٔ دیگر را دریافت کند یا برای آن ارسال کند (بنابراین اطلاعات در سطح شبکه پخش می‌شود و برای اشخاص ثالث پخش نمی‌شود).

9. Altering
10. Transmogrify
11. Karthikeyan

سایبری تاریخ یا محتوای فایل یا داده را تغییر می‌دهد. برای مثال، با دانستن آن‌که فایل Plan.jpg مظنون دستگاه قضا قرار گرفته است، اطلاعات یا تاریخ این فایل را تغییر می‌دهد. اما در تغییر شکل (فرمت)، هدر[1] فایل یا عنوان را تغییر می‌دهد. مثلاً فایل مذکور را به Plan.pdf تغییر فرمت می‌دهد! با این کار، محقق فارنزیک که دستور قضایی مبنی بر تفتیش داده‌های تصویری داشت، دیگر نمی‌تواند دلیل مجرمانه را بیابد.

۲-۵-۴. حملات علیه دیجیتال فارنزیک و ابزارهای آن

این روش اخیراً در میان مجرمان سایبری شکل گرفته است. در این روش، به‌جای حذف داده‌ها و مبهم‌سازی آن‌ها، ابزارهای فارنزیک هدف قرار می‌گیرند. متخصصان فارنزیک ابتدا برای آن‌که ادلهٔ موجود در وسیلهٔ دیجیتال مورد تهاجم قرار نگیرد از آن تصویر یا کپی می‌گیرند. این کار سبب می‌شود که مجرمان سایبری با نرم‌افزارهای مدرن خود هش (hash)[2] ارسالی از طرف متخصصان را تغییر می‌دهند، ازاین‌رو دیگر ادلهٔ به‌دست‌آمده را غیرقابل اعتماد[3] می‌سازند (Shanmugam, 2011, p.32).

۳. موضع نظام کیفری ایران و انگلستان در مواجهه با فارنزیک و آنتی‌فارنزیک (تفسیر قابل‌دفاع)

۳-۱. رابطهٔ نظام تحصیل دلیل با دلیل در دو نظام کیفری

میان نهاد تحصیل دلیل و نهاد دلیل و اثبات دلیل در امور کیفری و مدنی رابطه‌ای تنگاتنگ وجود دارد. بدین معنا که هرگاه تعداد دلیل‌ها محدود باشند نظام کیفری، در راستای تضمین عدالت کیفری، راه تحصیل دلیل را گسترش می‌دهد. به‌نظر می‌رسد نظام آرمانی راه دیگری در برقراری تعادل میان این دو نهاد ندارد. به فرض، اگر دلایل عبارت باشند از x و y، با توجه به مصلحت عامه، تحصیل دلیل به راه‌هایی از قبیل z,n,m,v گسترش می‌یابد. این مبنا دلایل گوناگونی دارد که مهم‌ترین آن‌ها عینیت‌نبخشیدن به دلایل است. به عبارت دیگر، دلایل از صورت ذهنی و شخصی قاضی باید خارج شوند و قالبی نوعی و عینی به خود بگیرند.

عینی‌سازی مستندات تحصیل دلیل شاخصه‌های منحصربه‌فردی دارد؛ ازجمله آن‌که برای اشخاص جامعه نوعی اطمینان حقوقی[4] ایجاد می‌کند. این اطمینان حقوقی دیگر به چالش با فرض ضعیف «جهل به قانون عذر نیست»[5] نخواهد رفت. دوم آن‌که بستر حمایت‌های حداکثری و یکسان‌سازی قوانین و قواعد جامع را فراهم می‌کند. سوم آن‌که شخص متهم، در صورت مجرم شناخته‌شدن، خود را از حیث اخلاقی نیز سرزنش می‌کند و از این جهت به بهبود شخصیت بزهکار و جامعه کمک می‌کند. چهارم آن‌که خسارات کمتری به اشخاص وارد می‌شود. در آخر، باب سوءاستفادهٔ بعضی قضات و ضابطان دادگستری بسته خواهد شد.

باید توجه داشت که آنچه در تعریف دلیل و انواع آن بیان شد هم درخصوص وهلهٔ پیش از تحصیل دلیل و در ارتباط با جرائم غیرمشهود و مشهود در مواد ۴۴ و ۴۵ آیین دادرسی کیفری صادق است و هم در رابطه با پس از تحصیل دلیل در مقام صدور رأی. در واقع رویکردی که مقامات عالی به دلایل دارند به‌ناچار درخصوص افسران و ضابطان دادگستری تأثیر می‌گذارد. برای مثال، در حقوق انگلیس اگر دستور تفتیش منزل از جانب مقام عالی صادر نشود، ضابط حق بررسی منزل مسکونی را ندارد (در حقوق ایران نیز به همین قرار است).[6] به‌هرحال، با توجه

---

1. Header

۲. این اصطلاح در علم کامپیوتر به معنای روشی است که برای یک‌دست‌بودن داده‌ها به‌کار می‌رود. برای مثال، اگر داده‌های ما قبل از انتقال دست‌برد زده نشده باشد و تغییری در آن ایجاد نشده باشد هش ارسالی ما با هش دریافتی ما یکسان خواهد بود والا تغییر می‌کند.

۳. اما غیرمعتبر (inadmissible) نمی‌سازند.

4. Legal certainty

۵ Ignorantia juris non excusat؛این مورد اخیراً موضوع بحث و مناقشهٔ بسیاری از حقوق‌دانان قرار گرفته است که آیا جهل به قانون، آن‌هم در قرن ۲۱، عذر نیست؟ تا جایی که دانشگاه خنت بلژیک در مورد موضوع مذکور بورسیهٔ مقطع دکتری اختصاص داد.

٦. بند ۴ مادهٔ ۱ قانون پلیس و ادلهٔ کیفری ۱۹۸۴ Police and Criminal Evidence Act 1984

به مطالبی که تاکنون بیان شد، بازخوانی روشنی از مادهٔ ۶۷۲ دادرسی کیفری (آیین دادرسی جرائم رایانه‌ای) درخصوص تحصیل دلیل دیتا دیجیتال به‌دست می‌رسد.

این ماده مقرر می‌دارد: تفتیش و توقیف داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی در حضور متصرفان قانونی یا اشخاصی که به نحوی آن‌ها را تحت کنترل قانونی دارند نظیر متصدیان سامانه‌ها انجام می‌شود. درصورت عدم‌حضور یا امتناع از حضور آنان، چنانچه تفتیش یا توقیف ضرورت داشته باشد یا فوریت امر اقتضا کند، قاضی با ذکر دلایل دستور تفتیش و توقیف بدون حضور اشخاص مذکور را صادر می‌کند.

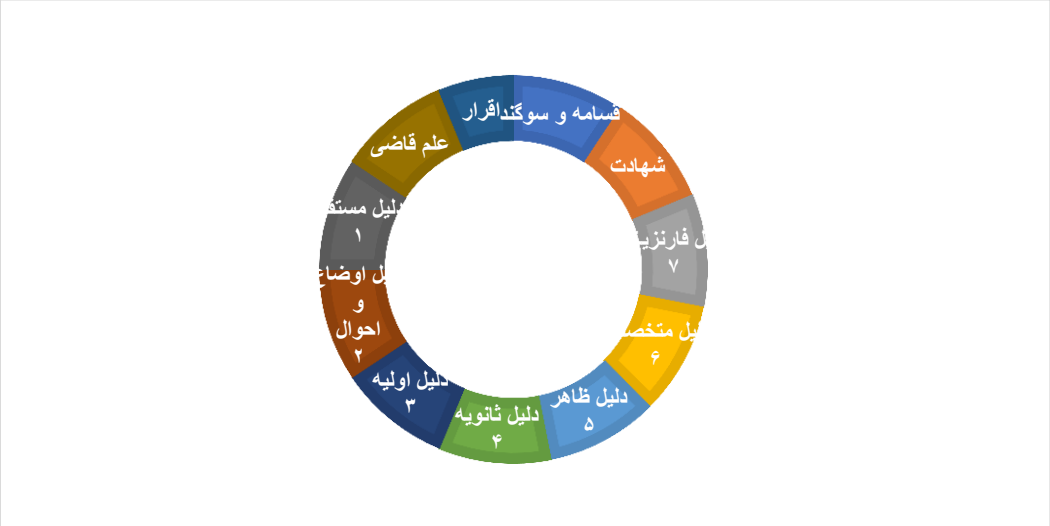
آیین دادرسی جرائم رایانه‌ای مانند دادرسی جرائم فیزیکی هنوز در توضیح و تعریف دقیق دلیل منطقهٔ فراغی را برای خواننده ترسیم می‌کند. مراد از دلایل آیا دلیل اولیه است یا ثانویه؟ دلیل ظاهر است یا متخصص؟ دلیل علمی (فارنزیک/ سایتیفیک) یا متخصص؟ یا همان‌گونه که مادهٔ ۶۷۱ آیین دادرسی کیفری بیان می‌کند، تفتیش و توقیف داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی به‌موجب دستور قضائی و در مواردی به‌عمل می‌آید که ظن قوی به کشف جرم یا شناسایی متهم یا ادلهٔ جرم وجود دارد.

باید دقت کرد که مواد مذکور دربارهٔ تحقیقات مقدماتی است و از این حیث با قواعد حقوق انگلیس نیز مشابه است. حقوق انگلیس نیز مقام تعقیب را موظف به فراهم‌آوری دلایل واقعی (Realistic) کرده است. اما آیا در فضای مجازی می‌توان با توجیه مصلحت عامه ظن قوی یا دلایل واقعی را توجیه کرد؟ دلایلی که هیچ معیار عینی ارائه نمی‌دهند. درمقابل، شکی وجود ندارد که فضای مجازی حاوی محتوای سرّی برای هر دارندهٔ وسیلهٔ دیجیتال به‌شمار می‌رود. امروزه اشخاص مهم‌ترین اطلاعات مرتبط با زندگی شخصی خود را در گوشی، ایمیل و لپ‌تاپ ذخیره می‌کنند. آیا با رویکرد مادهٔ ۶۲۷ قانون دادرسی کیفری و بدون تمییز جرایم صورت می‌پذیرد. تصور کنید الف (دانشمند هسته‌ای) پدر ب (سارق مسلح) اسرار تجاری را در ایمیل خود ذخیره کرده است. مقام قضایی با ظن قوی به این موضوع که پیام‌هایی از سوی ب در ایمیل شخصی الف وجود دارد دستور توقیف[1] ایمیل‌های الف را می‌دهد؛ در اینجا اسرار تجاری به‌موجب تبصرهٔ ب مادهٔ ۳۸ آیین‌نامهٔ جمع‌آوری و استنادپذیری ادلهٔ الکترونیکی (مصوب ۱۳۹۳) تکثیر می‌شود. به زبان ساده، بر روی دیسکت، تراشه یا فایل دیجیتالی که مأمور دادگستری تهیه کرده است کپی می‌شود. با این وصف، اسرار تجاری الف نزد مأمور باقی می‌ماند و اگر از تصرف او ربوده شود ضرر غیرقابل جبرانی به الف می‌رسد. دومین اشکال این است که اسرار تجاری برای مدت نا محدود دست مأمور باقی خواهد ماند! حتی پس آن‌که مأمور از وضعیت استخدامی خارج شود، فایل به بقای خود ادامه می‌دهد. بروز این‌همه ضرر (اعم از معنوی و مادی) ناشی از عبارت ذهنی «ظن قوی» در مادهٔ ۶۷۱ ق.ا.د.ک است.

اما این انتقاد به حقوق انگلیس وارد نیست. زیرا، به‌موجب قانون حمایت از داده‌ها (مصوب ۲۰۱۸) با بهره‌گیری از مقررات عمومی حفاظت از داده‌ها-مقررهٔ اتحادیهٔ اروپا (۲۰۱۸)، گرچه ملاک معقول‌بودن را محدود نساختند، از ورود ضرر با ایجاد محدودیت زمانی و حذف اتومات و... جلوگیری کرده‌اند.

به‌نظر می‌رسد که اگر دلایل در مرحلهٔ صدور رأی عینی شود، قضات با نگاه به همان دلایل دستور تحصیل دلیل را صادر می‌کنند. چرا که دلیل باید محکمه‌پسند باشد و اگر مقام قضایی بدواً بداند که پنجاه درصد امکان آن وجود دارد که دستور تحصیل دلیل وی به تکمیل پرونده در دادسرا یا تکمیل تحقیقات آن در دادگاه منجر نشود، عملاً از صدور دستور امتناع می‌ورزد. ازاین‌رو عینی‌بخشی دلیل بر عینیت‌بخشی به تحصیل دلیل اثرگذار است.

1 .Warrant of seizure



شکل ۱:عدم توازن در دو نظام ادله

در شکل ۱، عدم‌توازن ادله در دو نظام حقوقی ایران و انگلیس نشان داده شده است. تفاوت اصلی در علم قاضی یا امارات قضایی است که در حقوق انگلیس در ذیل دسته‌بندی‌های عینی قرار می‌گیرد، اما در حقوق ایران حدود و ثغوری برای علم قاضی درنظر گرفته نشده است. برای مثال، اگر قاضی سگ اهلی دارد که بوی مواد مخدر را تشخیص می‌دهد و با واردشدن متهم سگ پارس کند یا به او حمله‌ور شود، در اینجا ممکن است قاضی وفق نظام حقوق کیفری ایران علم شخصی حاصل کند.

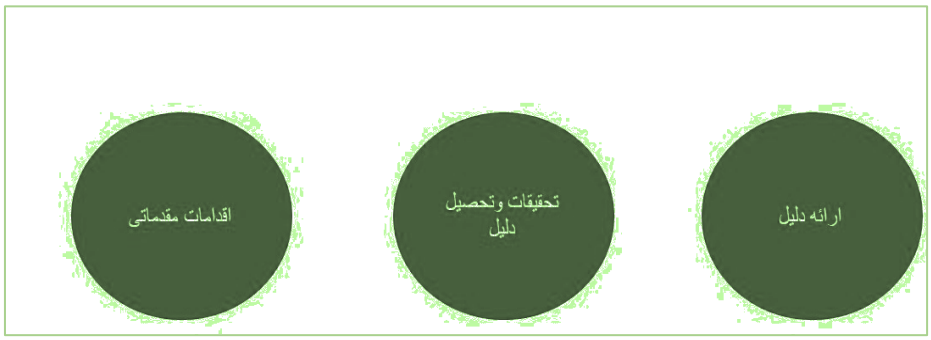
۳-۲. فرایند فارنزیک در دو نظام کیفری انگلستان و ایران

سازوکار تحصیل ادله در مقام بازداشت موقت یا به‌عبارتی پی‌بردن به متهم‌بودن شخص با مرحلهٔ مجرمیت در هردو نظام حقوقی ایران و انگلستان یکسان است. بنابراین، ادله‌ای که در مقام تحقیق به‌دست می‌آید و مبنای آن شخصیت بد متهم[1] یا ظن قوی باشد، در مرحلهٔ پیش از رسیدگی توسط قاضی کاربرد خواهند داشت. اما قاضی دادگاه بر اساس ادله‌ی موجد ظن مذکور نمی‌تواند رأی خود را صادر کند. برای مثال، اگر متهم تصادف بزرگی کرده است و دلیلی مبنی بر مصرف الکل توسط وی وجود دارد، گرچه این دلیل در مرحلهٔ تعقیب و تحقیق پذیرفته می‌شود، بدون علم به میزان مصرف، قاضی رأی صادر نمی‌کند. در مقابل، اگر دلیلی (مانند شاهد) مبنی بر مصرف کوکائین توسط الف یافت شود، در هردو مرحلهٔ تحقیق و صدور رأی نیازی به دلیل عالم به میزان مصرف نخواهد بود.[2] علت آن است که دلیل اول مرتبط[3] با موضوع نیست اما دلیل دوم شرط ارتباط را دارد (Keane & McKeown, 2012, p.25). حتی توقیف اشیا و تفتیش آن نیز در حقوق انگلستان با معیار معقول‌بودن همراه است. در بند ۲ مادهٔ ۱ قانون پلیس و ادلهٔ کیفری مصوب ۱۹۸۴،[4] چنین مقرر شده است: «پلیس حق دارد ۱. هر شخص یا وسیلهٔ نقلیه‌ای را تفتیش کند؛ ۲. هرچیزی را که داخل وسیلهٔ نقلیه است برای یافتن وسیله یا شیء گم‌شده بررسی کند؛ ۳. می‌تواند شخص را به‌منظور بررسی مذکور توقیف کند.» اما در مادهٔ بعد این حکم را چنین تخصیص می‌زند: اگر از ظاهر چنین برداشت شود که ۱. نیازی به تفتیش نیست و ۲. تفتیش کاربردی نیست، پلیس نباید تفتیش کند.

1. Bad character
2. R v Pleydell [2006] 1 Cr App R 212, CA
3. Relevant
4. Police and Criminal Evidence Act 1984

بنابراین می‌توان سه مرحله برای تحصیل دلیل تصور کرد: ۱. اقدامات پیش از تحصیل دلیل؛ ۲. اقدامات حین تحصیل؛ ۳. اقدامات پس از تحصیل دلیل. اقدامات پیش از تحصیل دلیل مانند فراهم‌آوری زیرساخت‌ها برای جلوگیری از آنتی‌فارنزیک که اصطلاحاً آنتی‌آنتی‌فارنزیک نام دارد، اقدامات حین تحصیل دلیل مانند توقیف،[1] ذخیره‌سازی، طبقه‌بندی، آنالیزکردن. اقدامات پس از تحصیل دلیل مانند حذف ادلهٔ غیرمرتبط.

پس فرایند تحقیقات (دیجیتال فارنزیک) دارای سه مرحلهٔ ذیل است:



شکل ۲: مراحل دیجیتال فارنزیک

گرچه هنوز استاندارد جامعی برای هریک از این سه مرحله تهیه نشده است و از سال ۲۰۰۱ تا ۲۰۱۲ روش‌های مختلفی را برای فرایند دیجیتال فارنزیک پذیرفتند (Adams, 2019, p.119). برای نمونه، فریلینگ و شویتای، در اثر خود به نام مدل پردازش مشترک و همگانی، فرایند فارنزیک را به سه مرحلهٔ پیش از حادثه،[2] فاز آنالیز و تحقیقات[3] و فاز پساآنالیز[4] تقسیم می‌کنند (Freiling & Schwittay, 2007, p. 13). در فاز پیش از حادثه، سه دستورالعمل را لحاظ کرده‌اند: تشخیص حادثه[5] اولین پاسخ از سوی تیم فارنزیک[6] و طراحی راهبرد پاسخ.[7]

در فاز دوم، نحوهٔ آنالیز داده را شامل این مراحل می‌دانند: پاسخ زنده،[8] تصویربرداری یا تکثیر دیجیتال،[9] بازیابی داده‌ها،[10] برداشت ادله و نهایتاً کاهش و سازمان‌دهی.[11] در آخرین فاز، دو وظیفه را برعهدهٔ متخصصان می‌داند: گزارش‌دادن[12] و ایضاح مطالب (روشن بیان‌کردن مطالب برای افراد غیرمتخصص)[13] در حین گزارش.

کارگروهی دیگر نوشتار خود را جامع گزارش‌های پیشین تلقی کرده و بر این باور است که مقتضیات قانونی و حقوقی در فرایند ارائه‌شده توسط ایشان رعایت شده است. ایشان بیان می‌کنند که سه مرحله در تحقیقات وجود دارد:

الف) مرحلهٔ اقدامات مقدماتی: در این مرحله باید اقدامات زیر رعایت شود (Köhn et al., 2006):

۱. استانداردهای ارگان مرتبط

۲. دادرسی و سیاست‌های مربوطه برای کمک به تحقیقات

۳. آموزش

---

1. Seizure
2. Pre-incident
3. Analysis Phase
4. Post-Analysis Phase
5. Detection of Incidents
6 .Initial Response
7. Formulation of Response Strategy
8. Live Response
9. Forensic Duplication
10. Data Recovery
11. Harvesting
12. Report
13. Resolution

۴. مشاورهٔ حقوقی
۵. اطلاع‌رسانی به مراجع ذی‌صلاح
۶. طبقه‌بندی حوادث (حملات سایبری) گذشته
۷. طراحی راهبرد
ب) مرحلهٔ تحقیقات سایبری باید شامل موارد ذیل باشد:
۱. تشخیص و انتساب ادله در رایانه
۲. جمع‌آوری ادله از رایانه (مراد تهیهٔ نسخهٔ پشتیبان)
۳. انتقال ادله به محیط امن (مراد همان نسخهٔ دوم است)
۴. نگاه‌داری ادله در صحنهٔ وقوع جرم (نسخهٔ اول)
۵. بررسی ادله با استفاده از ابزار مناسب (یافتن ادلهٔ مجرمانه)
۶. آنالیز (نگاه‌کردن به نتیجه و محصول بررسی در مرحلهٔ ۵ برای تمایز ادلهٔ باارزش و معتبر از غیرمعتبر)
پ) مرحلهٔ نهایی (ارائه) باید شامل دو گام باشد:
۱. گزارش
۲. اثبات

اظهارنظر و ارائهٔ استانداردی درخصوص این موضوع نیازمند اطلاعات کافی دربارهٔ تمامی جرائم سایبری است. نمی‌توان گفت که فریلینگ و شویتای، که بدواً پاسخ فارنزیک را لازم می‌دانند و بعد تهیهٔ راهبرد را سخنی غیرمنطقی ایراد کرده‌اند، در مقابل کوهن که ابتدا طراحی راهبرد را لازم می‌داند، طرح جامع‌تری را ترسیم نموده‌اند. به‌نظر می‌رسد جرائم سایبری و انواع آنتی‌فارنزیک‌های به‌کار گرفته‌شده و مجرمان سایبری در هر مرحله تفاوت می‌کنند و شاید نتوان نقشهٔ راه جامعی برای تمامی حملات سایبری طراحی کرد.

بااین‌حال، قدر متیقنی توسط بعضی نظام‌های‌های حقوقی پذیرفته شده است. برای نمونه، انجمن افسران ارشد پلیس انگلستان در سال ۲۰۱۱ دستورالعملی را درخصوص جزئیات فرایند فارنزیک تهیه کرد که شامل قواعد، راهبرد، به‌دام‌انداختن ادله، آنالیز و ارائه است. در تاریخ ۱۳۹۳/۵/۱۲ مصادف با ۳ آگوست ۲۰۱۴، آیین‌نامهٔ جمع‌آوری و استنادپذیری ادلهٔ الکترونیکی توسط قوهٔ قضاییه با بخش‌هایی چون جمع‌آوری ادله، حفاظت از ادله و ارائهٔ ادله تصویب شد. اما عدم دقت کافی در تدوین این آیین‌نامه هریک از مواد آن را محل بحث نموده است.

۳-۳. متخصص فارنزیک یا ضابط دادگستری؟

در نظام کیفری ایران، ضابط مخصوص در امور دیجیتال فارنزیک پیش‌بینی نشده است. مادهٔ ۱۳ آیین‌نامهٔ جمع‌آوری ادلهٔ الکترونیکی مقرر می‌دارد: «در موارد مقتضی، اجرای دستور حفاظت با نظارت ضابطان قضایی متخصص یا اشخاص خبرهٔ موردوثوق به نمایندگی از طرف مرجع قضایی صورت انجام می‌شود» این ماده در مقام بیان موارد نادر است، که در واقع از منظر قانونگذار رواست و در واقعیت هم به دلیل کمبود منابع متخصص اقتضای چنین امری بعید نیست. مواد ۲۴، ۳۴،۳۶، ۳۹ و ۴۳ نیز به تفاوت میان ضابط متخصص و ضابط ساده اشاره می‌کند. شاید اشکال شود که مادهٔ ۳۶ پاسخ ایراد را داده است؛ آنجا که مقرر کرده: «ضابطان و اشخاصی که حسب قانون مأمور جمع‌آوری، تفتیش، نگه‌داری، حفظ و انتقال داده‌ها و سامانه‌های رایانه‌ای یا مخابراتی می‌شوند باید علاوه‌بر داشتن شرایط لازم از قبیل تخصص و توانایی فنی و آموزش کافی، تجهیزات و وسایل لازم را در اختیار داشته باشند». اما، نخست این‌که میان متخصص فارنزیک یا همان سایتفیک که به زبان فارسی یعنی دانشمند با شخصی که مهارت لازم در جمع‌آوری داده را دیده تفاوت است؛ دوم این‌که نیاز به متخصص فارنزیک به دلیل اقدامات آنتی‌فارنزیک حتی در مرحلهٔ جمع‌آوری و نگاه‌داری داده لازم است، زیرا پیش‌تر بیان شد که به‌راحتی با حمله‌ی سایبری، مانند

حملات علیه ابزار فارنزیک، حفظ ادله ناممکن می‌شود. سوم، با توجه به این‌که در هیچ قسمت از آیین‌نامه سخنی از تخصص مأمور به‌میان نیامده است، به‌نظر می‌آید قانونگذار در همان عادت پیشین خود وفادار مانده و در فضای فیزیکی جمله را به‌کار برده است و مراد تخصص در توقیف و حفاظت فیزیکی است یا حفاظت حداقلی (مانند انتقال داده‌ها از لپ‌تاپ به دیسکت) که اساساً از عبارت تخصص به‌صورت مجازی استفاده کرده است. اما در همین قسمت لازم است به دستورالعمل افسران ارشد پلیس انگلستان توجه کرد. در مادۀ ۱٫۲ این دستورالعمل، محدودۀ اعمال چنین مشخص می‌شود:

«... اشخاصی که در زمینۀ بازیابی داده‌ها و توقیف آن‌ها همکاری می‌کنند، در صورتی که آموزش در این خصوص دیده باشند و با این شرط که دورۀ آموزشی در بخش مربوطه دربارۀ ارائۀ دلیل در دادگاه را گذرانده باشند. اشخاصی که دورۀ آموزشی ندیدند و شرایط ایشان با قواعد این دستورالعمل مطابقت ندارد، نمی‌توانند این موضوع از فعالیت را عهده‌دار شوند...»[1]

با توجه به این ماده، دو اشکال درخصوص فرایند دیجیتال فارنزیک ایران، در مقایسه با نظام حقوقی انگلیس، به ذهن خطور می‌کند؛ اول این‌که لزوم مهارت متخصص در ارائه و توضیح آنچه دیده است در محضر قاضی از لازمه‌های تعریف فارنزیک است. درحالی‌که در آیین‌نامه و همچنین آیین دادرسی جرائم رایانه‌ای این موضوع نادیده انگاشته شده است. علت آن است که دلیل متخصص،[2] که سابقاً در فصل اول بدان پرداخته شد، در حقوق ایران پذیرفته نشده است؛ بلکه دلیل متخصص در ایران در حد امارۀ قضایی دیده می‌شود و مجدد به همان سخن اول برمی‌گردیم که لزوم طبقه‌بندی و دسته‌بندی امارات قضایی است. رویکرد حقوق ایران، به دلیل آن‌که بهای بیش از حد به علم قاضی داده است، در سازوکار تحصیل دلیل نوین نیز دچار مشکلات عدیده‌ی ناشی از رابطۀ تحصیل دلیل با دلیل می‌شود. دوم این‌که متخصص باید علم و مهارت کافی در توقیف، بازیابی اطلاعات و داده‌ها، و فرایند آنتی‌آنتی‌فارنزیک را نیز داشته باشد. این امر کاملاً از نظر قانونگذار ایرانی به دور مانده است. گویی وظیفۀ متخصص صرفاً حفاظت فیزیکی از سخت‌افزار، دیسکت یا تراشه است. سوم این‌که متخصص باید از داخل ارگان باشد نه از خارج ارگان مسئول بازرسی. مورد اخیر هنوز ضعف بسیاری از قوانین موجود است.

۳-۴. مکان پردازش داده‌ها

در تحقیقی که از ادارات پلیس ایالت تگزاس انجام شد (Belshaw, 2019, p. 8)، این سؤال مورد پرسیده شد:

آیا ادارۀ شما توانایی دارد که ادلۀ دیجیتال را در خود اداره پردازش کند یا برای این کار باید داده‌ها را به آزمایشگاه‌های بیرون از اداره بفرستید؟

- شانزده اداره نظر دادند که فرایند پردازش کاملاً داخلی است و به خارج ارسال نمی‌شود.
- پانزده اداره گفتند که فرایند پردازش را در آزمایشگاه‌های خارج از اداره انجام می‌دهند.
- یازده اداره به‌صورت مختلط (داخل و خارج) پردازش می‌کنند؛ گاهی در اداره پردازش می‌کنند و گاه داده را به بیرون از اداره می‌فرستند.

مادۀ ۳۵ آیین‌نامه برای تکمیل ویژگی محرمانگی مقرر داشته است: «تفتیش داده‌ها یا سامانه‌ها در محل استقرار یا از طریق شبکه یا در آزمایشگاه یا در محل مناسب با دستور و تشخیص مقام قضایی با رعایت صحت، تمامیت، محرمانگی، و انکارناپذیری ادله انجام می‌پذیرد». بااین‌همه، حفظ محرمانگی در جایی که داده‌های شخص ثالث نیز درگیر مراحل تحقیق و تفتیش بازرسان باشد توجهی بیشتر از جانب قانونگذار می‌طلبد. برای مثال، اگر مقام قضایی ظن قوی داشته باشد (مادۀ ۶۷۱ قانون آیین دادرسی کیفری) که ایمیل شخص الف (تاجر خوش‌نام) دارای پیام‌هایی از جانب شخص ب (متهم) است که به رمزگشایی داده‌های مکشوفه منجر می‌شود، با توجه به آن‌که پیام‌های

1.https://www.npcc.police.uk/documents/crime/2014/Revised%20Good%20Practice%20Guide%20for%20Digital%20Evidence_Vers%205_Oct%202011_Website.pdf (Last visited on 11/13/2022)
2. Expert evidence

شخصی الف حاوی منافع مادی و معنوی است، متصرف این داده‌ها چه کسی خواهد بود؟ ضابط ساده؟ یا متخصص؟ و در چه مکانی این محتوا نگاه‌داری خواهد شد؟ در چه دستگاهی دادهٔ توقیف‌شده حفاظت شود؟ فیزیکی یا دیجیتالی ذخیره شود؟

۳-۵. نحوهٔ توقیف داده‌ها

تبصرهٔ مادهٔ ۳۸ در همین خصوص بیان داشته است: «توقیف باید حتی‌الامکان بدون ایجاد مانع برای فعالیت سامانه و به روش ساده و کم‌هزینه به شیوه‌هایی از قبیل ذخیره در حامل‌های داده، ذخیره در سامانه با گذاشتن گذرواژه، تهیهٔ نسخهٔ پشتیبان، تصویربرداری، تهیهٔ رونوشت و چاپ انجام شود». با توجه به تبصرهٔ مادهٔ ۳۸، آنچه در آیین‌نامه برای مقنن اهمیت دارد ساده‌بودن روش و کم‌هزینه‌بودن است. درحالی‌که مقنن می‌توانست محدودهٔ حجمی برای داده‌ها تعیین کند. برای مثال، حجم بیشتر از یک گیگ دیجیتال و کمتر از یک گیگ فیزیکی ذخیره شود. نگارش مادهٔ مذکور سه ایراد جدی حقوقی دارد: اولاً ماده باید مصلحت مهم‌تر را درنظر داشته باشد. حفظ داده در محیط ایمن ملاک و معیار است نه ارزان‌بودن یا ساده‌بودن. دوم این‌که قانونگذار خود را درگیر مسائل جزئی نمی‌کند.[1] با اغماض از ارزان‌بودن، که ملاک آن درخصوص فایل یک کیلوبایتی مشخص نیست، درخصوص معیار ساده‌بودن، قانونگذار چه معیاری در ذهن داشته است؟ آیا ساده‌بودن به معنای آسان‌بودن برای ضابطان است؟ توقیف به‌هیچ‌وجه نباید برای همیشه باشد، درحالی‌که قانونگذار ایرانی برخلاف قانونگذار انگلیسی زمان حذف را مشخص نکرده است. ظاهر آن است که ضابط بعد از توقیف نیز از نسخهٔ پشتیبان بهره‌مند می‌شود! اشکال دیگری که درخصوص نظام تحصیل دلیل دیجیتال ایران وجود دارد آن است که داده‌های غیرمرتبط در فرایند توقیف از نسخهٔ پشتیبان حذف نمی‌شوند. در مقابل، مطابق مادهٔ ۲ (b) و بند ۲ و بند ۵ مادهٔ ۱۵۱ و سایر مواد قانون حمایت از داده‌ها (۲۰۱۸)، باید داده‌های شخصی بلافاصله از نسخهٔ پشتیبان حذف شوند و مقرر می‌دارد که در این مسیر باید هرگونه گام معقول برداشته شود تا این اطمینان به‌دست آید که موارد غیرمرتبط با دستور مقام قضایی حذف شده است.

۳-۶. حذف داده‌های غیرمرتبط

اشکال دیگر که درخصوص نظام تحصیل دلیل دیجیتال ایران وجود دارد آن است که داده‌های غیرمرتبط در فرایند توقیف از نسخهٔ پشتیبان حذف نمی‌شوند. در مقابل، مطابق مادهٔ ۲ (b) و بند ۲ و بند ۵ مادهٔ ۱۵۱ قانون حمایت از داده‌ها (۲۰۱۸)، باید داده‌های شخصی بلافاصله از نسخهٔ پشتیبان حذف شوند و مقرر می‌دارد که در این مسیر باید هرگونه گام معقول برداشته شود تا این اطمینان به‌دست آید که موارد غیرمرتبط با دستور مقام قضایی حذف شده است.[2]

از جانبی دیگر، فارنزیک دیجیتال وظیفه‌ای قانونی بر عهده دارد که گرچه در تعریف لغوی آن پذیرفته نشده است اما به‌سبب اعمال قواعد غیرقابل انکار حقوقی این وظیفه بر عهدهٔ متخصصان این رشته است و آن حذف داده‌های غیرمرتبط است.[3] بی‌تردید این قسم جزو فاز سوم تحصیل دلیل به‌شمار می‌رود. البته نقض آن به معنای غیرمعتبر شناخته‌شدن دلیل نیست. ادلهٔ مجرمانه باید از ادلهٔ غیرمجرمانه به‌نحوی تصفیه شوند و ادلهٔ مجرمانه در پروندهٔ کیفری نگاه‌داری و دلیل غیرمجرمانه حذف شود. این مسئله غیر از بحث اخیر (حذف داده‌های غیرمرتبط) است، که با جست‌وجویی که در هردو نظام انجام شد مقرره و قاعده‌ای درخصوص آن یافت نشد. برای مثال، نامه شامل پتنت یا اسرار تجاری است و در انتهای نامه دلیل مبنی بر تجاوز به کودک وجود دارد. قسمت پتنت یا اسرار تجاری، که به‌صورت هارد کپی (hard copy) یا نسخهٔ فیزیکی در پرونده نهاده می‌شود، باید برای حفظ محرمانگی شطرنجی شود؛ مگر آن‌که حاوی استگانوگرافی یا پوچ‌نگاری باشد که تشخیص آن

1. De minimis non curat lex

۲. طرح حمایت و حفاظت از داده و اطلاعات شخصی (۱۳۹۹) نمونهٔ ایرانی GDPR اروپایی است که متأسفانه فاقد پیشنهادی درخصوص پاک‌کردن داده‌های غیرمرتبط است.

۳. مادهٔ ۳۹ قانون حفاظت از داده‌های انگلستان مقرر می‌کند پردازش داده‌ها باید مدت انتها داشته باشد و برای همیشه نباشد.

با متخصص فارنزیک است نه قاضی. با وجود این، در نظام قضایی ایران تشخیص نوع داده بر عهدهٔ قاضی نهاده شده است (مادهٔ ۶۷۳ آ.د.ک و بند الف مادهٔ ۳۷ آیین‌نامهٔ جمع‌آوری و استنادپذیری ادلهٔ الکترونیکی).

مؤید هرآنچه گفتیم در نظام کیفری ایران مادهٔ اخیر (مادهٔ ۳۷ آیین‌نامهٔ جمع‌آوری و استنادپذیری ادلهٔ الکترونیکی) است که بیان می‌دارد: هنگام تفتیش، شیوهٔ اقدام نباید به امحای داده‌ها منجر شود.

گویی داده‌ها مانند مجرم بالفعل‌اند که به‌هیچ‌وجه نباید ازدست بروند. حتی اگر حذف آن‌ها برای صلاح‌دید و حفظ صیانت و آبروی ثالث باشد، این عمل از منظر مقنن ممنوع است.

نتیجه‌گیری

همواره مجرمان واقعی، به‌سبب بیم دستگیری، شناسایی و توقیف ادلهٔ مجرمانه، اقداماتی برای محو و مبهم‌سازی مسیر دست‌یابی به دلایل انجام می‌دهند. در این اثر، با محوریت قراردادن تحصیل دلیل رایانه‌ای در دو نظام کیفری ایران و انگلستان، دست یافتیم که هیچ‌یک از اقدامات فنی‌حقوقی مقنن ایرانی در راستای تحصیل دلیل دیجیتال مطابق با تئوری‌های علمی حوزهٔ دیجیتال فارنزیک نیست. در این راستا توصیه می‌شود در قالب دستورالعمل حقوقی و فنی جمع‌آوری و استنادپذیری ادلهٔ الکترونیکی ۱۳۹۳ این مواد پیشنهادی درج شود:

۱. حذف تصویر اخذشده از سامانه یا داده باید فوری و به محض اتمام مدت تفتیش و توقیف صورت پذیرد

۲. ضابط و مأمور توقیف، از آن جهت که اطلاعات غیرمرتبط را حذف نکرده‌اند، باید مسئول جبران ضرر و زیان وارده به شخص ثالث و متهم فرض شوند.

۳. در صورت تشخیص ضابط فارنزیک مبنی بر نحوهٔ توقیف، کم‌هزینه‌بودن یا آسان‌بودن توقیف، که موضوع تبصرهٔ مادهٔ ۳۸ آیین‌نامهٔ جمع‌آوری و استنادپذیری ادلهٔ الکترونیکی (۱۳۹۳) است، به «آنچه در مقابل حملات سایبری تدوام دارد» قابل تغییر است.

منابع

آقایی، بهمن (۱۳۷۸). فرهنگ حقوقی بهمن. تهران: گنج دانش، چاپ اول.

ابوالمعالی الحسینی، سیدوحید (۱۳۹۵). قواعد تحصیل دلیل کیفری در فضای سایبر. رسالهٔ دکتری، پردیس فارابی دانشگاه تهران.

احمد بن فارس، ابی حسین (۱۴۰۴ه.ق). معجم مقاییس اللغه، جلد ۲. بی‌جا: مکتبه الاعلام الاسلامی.

السان، مصطفی (۱۳۹۹). حقوق فضای مجازی. تهران: مؤسسهٔ مطالعات و پژوهش‌های حقوقی شهردانش، چاپ چهاردهم.

بابایی، جواد (۱۴۰۰). جرایم رایانه‌ای و آیین دادرسی حاکم بر آن. تهران: معاونت امور فرهنگی قوهٔ قضاییه، چاپ ششم.

جعفرزاده، میرقاسم و عاکفی قاضیانی، وحید (۱۴۰۱). محصول دیجیتال به مثابه کالا در حقوق بیع بین‌الملل. مجله حقوق تطبیقی، ۱(۱۳)، ۱۶۵-۱۸۴.

حیدری، الهام (۱۳۹۳). اعتبار علم قاضی درصدور احکام کیفری در قانون مجازات اسلامی مصوب ۱۳۹۲. پژوهشنامه حقوق کیفری، ۵(۱۰)، ۱۱۰-۸۹.

عبدی‌پور، ابراهیم و وصالی، مرتضی (۱۳۹۶). توسعهٔ مفهوم و مصادیق مال در فضای مجازی. پژوهش تطبیقی حقوق اسلام و غرب، ۴(۱)، ۱۱۲-۸۵.

گلدوزیان، ایرج (۱۳۸۲). ادله‌ی اثبات دعوی. تهران: نشر میزان، چاپ دوم.

مدنی، جلال‌الدین (۱۳۷۸). آئین دادرسی کیفری ۱ و ۲، تهران: پایدار.

میرمحمدصادقی، حسین (۱۳۸۳). جرایم علیه اموال و مالکیت. تهران: نشر میزان، چاپ بیست‌وپنجم.

هاشمی شاهرودی، سید محمود (۱۳۷۸). بایسته‌های فقه جزا. تهران: نشر دادگستر.

یثربی، سیدعلی‌محمد (۱۳۸۵). بررسی علم قاضی در فقه و قانون. حقوق خصوصی، ۴(۱۱)، ۶۴-۷۲.

Adams, R. (2012). *The Advanced Data Acquisition Model (ADAM): A process model for digital forensic practice* (Doctoral dissertation, Murdoch University).

Anderson, T., Schum, D., & Twining, W. (2005). *Analysis of Evidence*, 2nd ed, UK: Cambridge University.

Belshaw, S. H. (2019). Next Generation of Evidence Collecting: The Need for Digital Forensics in Criminal Justice Education. *Journal of Cybersecurity Education, Research and Practice*, *2019*(1), 3. https://digitalcommons.kennesaw.edu/jcerp/vol2019/iss1/3

Conlan, K., Baggili, I., & Breitinger, F. (2016). *Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy*. *Digital Investigation*, *18*, S66-S75.

Del Carmen, R. V., & Hemmens, C. (2017) *Criminal Procedure Law and Practice*, 10th ed, USA: Cengage Learning.

Freiling, F., & Schwittay, B. (2007). A common process model for incident response and digital forensics. *Proceedings of the IMF2007*.

Hails, J. (2009). *Criminal Evidence*, 6th ed, Wadsworth Cengage Learning

Harris, R. (2006). Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. *digital investigation*, *3*, 44-49.

Jain, A., & Chhabra, G. S. (2014, August). Anti-forensics techniques: An analytical review. In *2014 Seventh International Conference on Contemporary Computing (IC3)* (pp. 412-418). IEEE.

Keane, A., & McKeown, P. (2012).*The Modern Law of Evidence*.UK: Oxford University Press, 9th ed.

Köhn, M., Olivier, M. S., & Eloff, J. H. (2006). Framework for a Digital Forensic Investigation .*Information and Computer Security Architectures Research Group (ICSA)* Department of Computer Science University of Pretoriamo.co.za/open/dfframe.pdf

Merriam-Webster. Inc (2003). *Merriam-Webster's collegiate dictionary*, Springfield, MA, 11th ed.

Moore, R. (2005). *Search and seizure of digital evidence* (p. 80). LFB Scholarly Pub.

Prasanthi, B. V. (2016). Cyber forensic tools: a review. *International Journal of Engineering Trends and Technology (IJETT)*, *41*(5), 266-271.

Shanmugam, K. (2011). *Validating digital forensic evidence* (Doctoral dissertation, Brunel University School of Engineering and Design PhD Theses).

Singh, C. (2022). *Unlocking the law of evidence*. NYC: Routledge, 4thed.

Singh, N. (2021). Recent Challenges in Digital Forensics. *ResearchGate*.

US-CERT (2008). *Computer Forensics*. https://www.cisa.gov/uscert/sites/default/files/publications/forensics.pdf

Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2021). Digital Forensics vs. Anti-Digital Forensics: Techniques, Limitations and Recommendations. *ArXiv, abs/2103.17028*.