Revija za kriminalistiko in kriminologijo / Ljubljana 72 / 2021 / 3, 219–232

Vpliv avtomatizacije digitalnih forenzičnih preiskav na dokazovanje v kazenskem postopku[1]

Liljana Selinšek[2]

Prispevek daje kratek vpogled v izzive in težave, ki jih je na področju digitalne forenzike prineslo vztrajno povečevanje števila elektronskih naprav in njihovih pomnilniških kapacitet, njihova vseprisotna uporaba in povezovanje ter s tem povezano veliko podatkovje. Digitalne forenzične preiskave danes pogosto zajemajo večje število naprav in ogromno količino podatkov, zaradi omejenih personalnih in tehničnih resursov pa v mnogih državah nastajajo preiskovalni zaostanki, ki negativno vplivajo na načelo sojenja v razumnem roku. Pri tem je vložek časa in sredstev v digitalno forenzično preiskavo v konkretnem primeru pogosto nesorazmeren z izsledki te preiskave, saj več naprav in podatkov ne pomeni nujno tudi več digitalnih dokazov, ampak le več materiala, ki ga je treba preiskati. Igla torej večinoma ostaja enaka, kopica sena, v kateri se jo išče, pa je čedalje večja. Ena od rešitev, ki se razvija za obravnavanje tega problema, je (delna) avtomatizacija digitalnih forenzičnih preiskav. V prispevku podajamo teoretično analizo trenutnega stanja na tem področju s posebnim uvidom v vprašanje, kaj avtomatizacija (strojna oziroma programirana preiskava) pomeni z vidika zanesljivosti rezultatov take preiskave za potrebe kazenskega postopka. Dokler ne bo na globalni ravni vzpostavljen koncept validacije in formalne verifikacije digitalnih forenzičnih orodij, ki bo vključeval merjenje njihove zanesljivosti, je pomembno, da imajo digitalni forenzični preiskovalci popoln nadzor nad vsemi fazami digitalne forenzične preiskave, odločevalci v kazenskem postopku (predvsem državni tožilci in sodniki) pa se morajo zavedati prednosti in pomanjkljivosti (delno) avtomatiziranih digitalnih forenzičnih orodij.

Ključne besede: digitalna forenzika, avtomatizacija v digitalni forenziki, digitalni dokaz, digitalizacija kaznivih dejanj, socializacija tehnologije, veliko podatkovje

UDK: 343.983.2:343.1

1 Uvod

V šestdesetih letih prejšnjega stoletja se je pojavila fraza, ki velja za eno bolj domiselnih šal[3] na področju sodobnih financ: »Najboljši način, kako oropati banko, je ta, da postaneš njen lastnik.«[4] Zdi se, da je tehnološki razvoj prinesel še boljšo možnost: »Najboljši način, kako oropati banko, je ta, da jo hekneš.«[5] V procesu vsesplošne digitalizacije naših življenj so tudi v plačilnem prometu postale prevladujoče elektronske transakcije. Namesto denarnice iz žepa tehnološko naprednejšim zmikavtom danes več obetajo uporabniško ime, geslo in identifikator za spletno bančništvo ali številka plačilne kartice, kar lahko za nameček pridobijo brez fizičnega stika z oškodovancem (npr. kar »na banki«). Nove kriminalne metode na drugi strani zahtevajo nove pristope pri odkrivanju in preiskovanju kaznivih dejanj, saj se klasičnim sledem pridružujejo digitalne sledi, ki ne ostajajo le za kibernetskimi, ampak tudi za čisto »navadnimi« (klasičnimi) kaznivimi dejanji. Ljudje se pogosto niti ne zavedamo, pri kako številnih, tudi čisto vsakdanjih, dejavnostih in opravkih puščamo za seboj digitalne sledi. Elektronske naprave so zato lahko nosilci dokazov v primeru najrazličnejših kaznivih dejanj, tudi takih, ki sama po sebi (glede na posledico) niso v ničemer povezana s kibernetskim prostorom. Z vseprisotnostjo tehnologije na vseh področjih življenja so se torej v pomembni meri »digitalizirala« tudi kazniva dejanja, za njihovo odkrivanje in preiskovanje pa potrebujemo čedalje boljšo opremo (strojno in programsko) in čedalje več znanja.

[1] Prispevek je nastal v okviru raziskovalnega projekta »Avtomatizirana pravičnost: družbeni, etični in pravni vidiki«, ki ga financira Javna agencija za raziskovalno dejavnost Republike Slovenije (št. projekta: J5-9347), izvaja pa Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani.

[2] Dr. Liljana Selinšek, docentka in raziskovalka na Inštitutu za kriminologijo pri Pravni fakulteti v Ljubljani, Slovenija. E-pošta: liljana.selinsek@pf.uni-lj.si

[3] Gre za šalo, ki ima v sebi tudi zrno resnice.

[4] V originalu »*The best way to rob a bank is to own one*«. Frazo je med drugim uporabil William Crawford, ki je junija 1987 pričal pred ameriškim Kongresom glede čedalje hujše krize na področju hranilništva in posojil.

[5] V angleščini bi se glasila »*The best way to rob a bank is to hack one*«. Google na dan oddaje tega prispevka (29. 6. 2021) fraze v svojem portfelju informacij ne najde, obstaja pa precej zapisov o načinih hekerskih napadov na banke.

Da lahko digitalna sled postane dokaz v kazenskem postopku, jo je treba poiskati in ustrezno shraniti, nato pa še analizirati v kontekstu primera, na katerega se nanaša, ter predstaviti odločevalcu. Navedeno – pridobivanje, ohranjanje, analiza in predstavitev digitalnih podatkov oziroma dokazov – je osnovno delovno področje digitalne forenzike (Homem, 2018; Larry in Lars, 2011). Digitalna forenzika se je začela razvijati pred približno petdesetimi leti in je bila v začetnih fazah omejena na obnovo (namerno ali po nesreči) izbrisanih podatkov (Caviglione, Wendzel in Mazurczyk, 2017), razmeroma hitro pa je postala orodje za aktivno iskanje dokazov. Najprej je digitalni forenzični proces obsegal le analizo posamezne elektronske naprave (enega računalnika ali mobilnega telefona), danes pa je zaradi hitrega tehnološkega napredka in t. i. socializacije tehnologije[6] v preiskavah le še redko zasežena le ena naprava (s pomnilnikom nekaj 10 gigabajtov), ampak so potencialni dokazi pogosto razpršeni prek več (medsebojno povezanih) elektronskih naprav (s pomnilnikom nekaj 10 *tera*bajtov).[7] Raznolikost elektronskih naprav in stalno naraščajo**ča** masa elektronskih podatkov v vsebinski, časovni in tudi personalni dimenziji zelo otežujeta digitalne forenzične preiskave. Več imamo podatkov, težje je zaznati goljufiva ravnanja in zlonamerne posameznike, ki jih opravljajo (Zawoad in Hasan, 2015). Poleg tega je za preiskavo potrebnega več časa in pogosto tudi več ljudi. Univerzalnih digitalnih forenzikov ni, saj noben preiskovalec nima (niti ne more imeti) specializiranega znanja, ki bi mu omogočilo preiskavo vseh vrst elektronskih naprav (Vincze, 2016). Posledično so digitalni forenzični preiskovalci širom po svetu zasuti z delom. Hkrati razvoj na pravnem področju zaostruje preiskovalne standarde, kar v končni fazi vodi do preiskovalnih zaostankov, lahko celo opustitve primerov (James in Gladyshev, 2013). Po podatkih iz leta 2018 v večini razvitih držav zaostanki pri izvedbi digitalnih forenzičnih preiskav znašajo v povprečju šest do dvanajst mesecev (Butterfield, Dixon, Miller in Schreuder, 2018), iz literature pa izhaja, da lahko zaostanki trajajo tudi do štiri leta (Lillis, Becker, O›Sullivan in Scanlon, 2016).[8] To resno vpliva na načelo poštenega sojenja, ki med drugim zahteva odločanje v razumnem roku.[9] Iskanje možnosti za izboljšave in pohitritev digitalnih forenzičnih preiskav tako ni le tehnično vprašanje oziroma potreba, ampak ima zaradi odvisnosti pravosodnega sistema in v njegovem okviru zlasti kazenskih postopkov od dokazov o izvedenem preteklem dejanju pomembne implikacije tudi v pravu; ob upoštevanju specialno in generalno-preventivne funkcije kazenskega prava mu lahko pripišemo (še) širši družbeni kontekst.

V pričujoči deskriptivni razpravi z uporabo metode *desk-research* preverjamo teoretične vplive programskih novosti pri izvajanju digitalnih forenzičnih preiskav na procese dokazovanja v kazenskem postopku. Pri tem se osredotočamo na čedalje aktualnejšo uporabo avtomatizacije[10] v digitalni forenziki, ki je še zlasti zanimiva (a tudi občutljiva), ker se v preiskavo neposredno vključi računalniški program oziroma algoritem. Zanima nas, ali se lahko z dokazno-pravnega vidika algoritmu prepusti del preiskave na način, da ta del preiskave prevzame; ali pa lahko algoritem glede na trenutno stanje razvoja digitalne forenzike kot (še ne docela?) znanstvene discipline del preiskave zgolj opravi (ne pa ga tudi prevzame). V iskanju odgovora na to vprašanje bomo v uvodu dali kratek vpogled v izzive, ki jih na področju digitalne forenzike prinaša veliko podatkovje, v nadaljevanju pa sledi razprava o nekaterih sistemskih vprašanjih, povezanih z izgradnjo zaupanja v rezultate digitalnih forenzičnih preiskav.

---

[6] Ta izraz se uporablja za medsebojno povezanost različnih elektronskih naprav, ki generirajo digitalne podatke.

[7] V letu 1990 so imeli računalniki v povprečju nekaj sto *mega*bajtov pomnilniškega prostora. V letu 2017 so denimo pametni telefoni že ponujali 128 gigabajtov prostora, računalniki in prenosniki pa diske z 2–4 *tera*bajti pomnilniškega prostora (Shalaginov, Johnsen in Franke, 2017). Ob tem obstajajo ocene, da ima v razvitem svetu vsak posameznik v povprečju pet omrež(e)nih elektronskih naprav, ki so lahko med seboj zelo različne (Vincze, 2016).

[8] Kar se tiče Slovenije, iz letnega poročila Policije za leto 2020 izhaja, da je policija v tem letu preiskala več kot 5.100 različnih e-naprav (od tega je bilo skoraj polovica prenosnih telefonov) in da se je pozitiven trend števila preiskav e-naprav nadaljeval tudi v tem letu, saj se e-naprave zasežejo v čedalje več predkazenskih postopkih (Ministrstvo za notranje zadeven, Policija, 2021). Uradnih podatkov o preiskovalnih zaostankih na tem področju ni, je pa iz zapisa v Skupnem poročilu o delu državnih tožilstev 2019, da na (daljše) trajanje predkazenskih postopkov med drugim vpliva zavarovanje in analiziranje večjega števila računalniških in drugih elektronskih naprav (Vrhovno državno tožilstvo, 2021), mogoče sklepati, da digitalne forenzične preiskave tudi v Sloveniji niso opravljene tekoče oziroma v zelo kratkih rokih.

[9] Skladno s 1. odstavkom 6. člena Evropske konvencije o človekovih pravicah (Svet Evrope, 1950) ima vsakdo med drugim pravico, da o kakršni koli kazenski obtožbi zoper njega pravično in javno ter *v razumnem roku* odloča neodvisno in nepristransko z zakonom ustanovljeno sodišče.

[10] Slovar slovenskega knjižnega jezika glagol »avtomatizirati« opredeljuje kot »s ponavljanjem povzročiti, da kaj poteka brez sodelovanja volje, zavesti« (Inštitut za slovenski jezik Frana Ramovša ZRC SAZU – Portal BOS, 2020). Nekoliko podrobneje Tehnopedia (2020) pojasnjuje, da avtomatizacija zajema razvoj in uporabo tehnologije z namenom proizvodnje in dostave različnega blaga in storitev z minimalnim sodelovanjem človeka. Implementacija avtomatiziranih tehnologij, tehnik in procesov izboljšuje učinkovitost, zanesljivost in/ali hitrost opravil, ki so jih prej izvajali ljudje. Avtomatizacija se uporablja na številnih področjih, kot so proizvodnja, transport, obramba, v zadnjem času pa tudi informacijska tehnologija.

2 Digitalna forenzika v dobi velikega podatkovja

Veliko podatkovje na številnih področjih prinaša koristi, na področju digitalne forenzike pa prinaša tudi različne izzive in težave. Forenzični strokovnjaki morajo nenehno spremljati napredek na tehničnem področju, kar je zahtevno samo po sebi, še večjo težavo v praksi pa predstavlja ogromna količina podatkov, ki jih je treba preiskati (Lopez, Moon in Park, 2016). Obstoječa orodja in infrastruktura ne morejo zagotoviti pričakovanega hitrega odziva, ko gre za preiskavo velike količine podatkov. Že pred približno desetletjem se je začelo ugotavljati, da čas, vložen v pregled stotine terabajtov podatkov, večinoma ni sorazmeren s količino najdenih digitalnih dokazov, dejansko relevantnih za konkreten primer. Razloga sta bila dva: čedalje večja količina informacij, ki jih je bilo treba preiskati, ter dejstvo, da forenzični preiskovalci iščejo sledi in dokaze po tradicionalnih, večinoma ročnih in časovno zahtevnih postopkih (Martuara, Tacconi, Berte in Me, 2012). Ko so se forenzični preiskovalci začeli soočati s težavami pri zbiranju, identifikaciji in analizi relevantnih dokazov iz velikih podatkovnih baz, se je začela znotraj digitalne forenzike kot posebna podpanoga razvijati t. i. forenzika velikega podatkovja (ang. *big data forensics*),[11] v okviru katere se obravnavajo različna vprašanja, ki so tehnične, proceduralne, sociološke in tudi pravne narave (Zawoad in Hasan, 2015).

V osnovi se je veliko podatkovje karakteriziralo s tremi značilnostmi: količina podatkov, raznolikost podatkov in hitrost obdelave podatkov (Qi, Liu, Lu, Liu in Li, 2014). Razvoj je dodal četrto značilnost – vrednost. Pri tem ni mišljena klasična finančna vrednost, ampak vrednost, ki jo podatki dobijo, ko se razkrijejo njihovi predhodno neznani vidiki oziroma različne možnosti uporabe. Nato se je pridružila še peta značilnost – verodostojnost, ki se nanaša na kakovost podatkov, na njihovo točnost, na upravljanje s podatki, pa tudi na varovanje zasebnosti in druga pravna vprašanja (Kishore, Saxena in Raina, 2017; Zawoad in Hasan, 2015). Vsaka od navedenih značilnosti velikega podatkovja na področju digitalne forenzike prinaša specifične izzive. Količina in hitrost se večinoma obravnavata s strojnimi in programskimi rešitvami, ki lahko v kratkem času obdelajo veliko količino podatkov, medtem ko na področju raznolikosti in verodostojnosti, ki med drugim obsegata nepopolne podatke in različne podatkovne formate, ni lahkih rešitev (Shalaginov et al., 2017). V nadaljevanju na kratko prikazujemo nekatere aktualne trende na področju digitalne forenzike, pri čemer se osredotočamo predvsem na vprašanje, ali (oziroma do kakšne mere) je sprejemljivo prepuščanje izvedbe (dela) digitalne forenzične preiskave avtomatiziranim forenzičnim orodjem oziroma računalniškim algoritmom.

2.1 Trenutni trendi v digitalni forenziki in uporaba avtomatizacije

Digitalna forenzika nikoli ni bila nezahtevno področje. Tudi pred pojavom velikega podatkovja so na tem področju obstajali številni (še vedno aktualni) izzivi: šifriranje, steganografija (skrivanje podatkov oziroma »zakrito pisanje«), obstoj antiforenzičnih orodij, raznolikost naprav in formatov podatkov, potreba po analizi nepopolnih, delno izbrisanih ali nekonsistentnih podatkov itd. (Adedayo, 2016; Lopez et al., 2016). Kot omenjeno, se navedenim, po naravi kvalitativnim izzivom v novejšem času pridružujejo še izzivi (težave) kvantitativne narave: naraščanje števila in pomnilniških kapacitet digitalnih narav, povečevanje količine podatkov, ki se lahko zberejo v povezavi s preiskavo, in potreba po hitri izvedbi oziroma hitrih rezultatih preiskave. Za rešitev teh težav raziskovalci razvijajo številne predloge in modele, ki segajo od čisto tehničnih (programskih)[12] pa do postopkovnih, zanimivih tudi s kazenskopravnega vidika.

Med postopkovnimi rešitvami sistemske narave je treba omeniti model, poimenovan »digitalna forenzika kot storitev« – ang. *Digital Forensics as a Service* (DFaaS). Gre za sodobno metodo upravljanja forenzičnega delovnega procesa, ki jo je v letu 2010 razvil Nizozemski forenzični institut kot odgovor na naraščajoče preiskovalne zaostanke. DFaaS je na oblaku temelječ model oddaljenega dostopa, ki preiskovalcem omogoča, da hitro pridejo do relevantnih digitalnih podatkov oziroma dokazov, saj se v preiskavo vključijo vsi razpoložljivi resursi posamezne organizacije. Model DFaaS temelji na tem, da se digitalni forenziki osredotočajo le na forenzične naloge, torej zaseg gradiva in pridobivanje podatkov iz njega, za ostala opravila pa se po potrebi vključijo drugi strokovnjaki (skrbniki aplikacij, skrbniki podatkovnih zbirk, pomnilnikov, infrastrukture ipd.). Digitalni podatki se pošljejo v centralizi-

[11] Izraz digitalna forenzika je danes v bistvu krovni izraz (ang. *umbrella – term*), ki vključuje številna podpodročja: računalniško forenziko, forenziko mobilne telefonije, pomnilniško forenziko, forenziko mrež, forenziko podatkovnih baz in metapodatkov (Shalaginov et al., 2017), GPS forenziko, forenziko socialnih omrežij, digitalno video in foto forenziko, forenziko digitalnih kamer, forenziko igralnih konzol, forenziko večosebnih računalniških iger (Larry in Lars, 2011) itd.

[12] Na primer rudarjenje po podatkih, filtriranje podatkov, uporaba statističnih tehnik za povezovanje podatkov na različnih pogonih (t. i. *cross-drive* analiza), uporaba umetne inteligence in inteligentnih analitičnih orodij, uporaba napredne podatkovne analitike. Iskanje rešitev na tehničnem področju se pogosto sicer osredotoča le na posamezno podfazo digitalnega forenzičnega procesa, v kateri v konkretnem primeru obstaja določen problem, kar pomeni, da gre bolj za *ad hoc* kot pa za sistemske rešitve na področju digitalne forenzike (Adedayo, 2016; Shalaginov et al., 2017).

ran sistem, ki samodejno izvleče sledi in digitalnim forenzikom, pa tudi preiskovalcem, ki vodijo primer, in analitikom omogoči dostop do teh sledi. Pri tem je za obdelavo primera mogoče uporabiti katero koli zmogljivost, ki je trenutno na voljo znotraj določene organizacije (ali celo med organizacijami, če se te povežejo). To omogoča, da se po potrebi aktivirajo rezervne zmogljivosti za skladiščenje in obdelavo podatkov, s katerimi razpolaga določena organizacija, ki lahko tako uporabi vso razpoložljivo procesorsko moč za pospešitev obdelave digitalnega gradiva. To je nato primarno na voljo preiskovalcem, ki vodijo primer. Ti za razliko od digitalnega forenzika primer poznajo in točno vedo, kaj iščejo oziroma potrebujejo. V tradicionalnem sistemu je digitalni forenzik dejansko posrednik, od katerega se pričakuje, da bo preiskovalcem, ki vodijo primer, zagotovil vse ključne informacije, čeprav primera v celoti sploh ne pozna. V sistemu DFaaS je zagotovljeno, da preiskovalci dobijo vpogled v vse sledi, sami lahko po teh sledeh iščejo in v nekaj sekundah filtrirajo pomembne podatke od nepomembnih. Če najdejo ustrezne zadetke, imajo neposreden dostop do izvornega gradiva, kot so slike, dokumenti in e-poštna sporočila. DFaaS izhaja iz tega, da mora biti digitalni material na voljo v prvih nekaj dneh preiskave, da se lahko uporabi tudi za oblikovanje preiskovalnih hipotez, kar v tradicionalnem digitalnem forenzičnem postopku ni izvedljivo, zaradi česar so sledi, najdene v digitalnem gradivu, pogosto uporabne le za preverjanje, namesto da bi bile ključne pri oblikovanju preiskovalne hipoteze. DFaaS torej pospešuje postopek preiskave tako, da preiskovalci dobijo digitalne podatke na razpolago v najkrajšem možnem času, kar jim omogoča, da jih maksimalno izkoristijo (van Baar, van Beek in van Eijk, 2014; van Beek, van Eijk, van Baar, Ugen, Boddle in Siemelink, 2015).

Dobro upravljanje forenzičnega delovnega procesa nedvomno pomembno pripomore k učinkovitosti digitalne forenzične preiskave, ne rešuje pa samo po sebi težav, povezanih z ogromno količino digitalnega preiskovalnega gradiva. Na tem področju se je s ciljem pohitritve preiskav razvil proces t. i. forenzične triaže, ki je namenjena temu, da se zmanjšata število naprav in posledično obseg podatkov, ki jih je treba preiskati. Gre za uvodno fazo digitalnega forenzičnega procesa (preliminarno preiskavo), v okviru katere se potencialni viri dokazov razvrščajo po pomembnosti oziroma prioriteti tako, da se zoži krog naprav in podatkov, ki jih je nato treba pregledati »ročno« oziroma z angažiranjem časa digitalnega forenzičnega preiskovalca (Marturana et al., 2012). S tem se do neke mere mehča t. i. načelo »*copy-all*«, ki je (bilo) eno osrednjih načel digitalne forenzike in (je) temelji(lo) na tem, da se za potrebe preiskave forenzično kopirajo in zasežejo prav vsi dostopni digitalni podatki. Namesto do pred kratkim »zlatega standarda«, to je polne preiskave vsebine vseh elektronskih naprav, ki so potencialni nosilci digitalnih dokazov, se po novem v zahtevnejših primerih, v katerih je količina elektronskih podatkov neobvladljiva, torej izvede preliminarna hitra analiza (Kishore et al., 2017), katere posebnost je ta, da večinoma poteka avtomatizirano.

Za avtomatizirane podprocese digitalnega forenzičnega procesa se je v literaturi pojavil izraz »forenzika na gumb« (ang. *push-button forensics*). Rešitev je na prvi pogled zelo obetajoča, a je razvoj razmeroma počasen in previden. Že pred desetletjem so avtorji ugotavljali, da se posamezne dejavnosti v digitalnem forenzičnem procesu sicer lahko avtomatizirajo, vendar je avtomatizacija zelo draga, učinek pa sorazmerno omejen (Garfinkel, 2010). Tudi iz novejše literature izhaja, da se digitalne forenzične preiskave še vedno v večjem delu izvajajo ročno oziroma so kvečjemu kvazi-avtomatizirane. Standardna forenzična orodja avtomatizirajo le nekaj predhodnih faz in imajo omejene zmožnosti povezovanja več dokaznih virov (Homem, 2018). Tudi na področju zelo razširjene forenzike mobilne telefonije se sorazmerno malo razpravlja o avtomatizirani klasifikaciji dokazov in avtomatizirani analizi obnašanja uporabnika. Oboje se še vedno večinoma izvaja ročno, razprave o avtomatizaciji teh procesov pa so za zdaj redke (Barmpatsalou, Cruz, Monteiro in Simoes, 2018).

Kmalu po pojavu forenzike na gumb so se začela pojavljati opozorila, da morajo biti ti procesi dobro načrtovani in predvsem pod nadzorom, saj lahko drugače pride do napak, ki si jih v kazenskem postopku ni mogoče privoščiti. James in Gladyshev (2013) sta argumentirano izpostavila naslednje:

— preiskave, ki temeljijo na visoki stopnji avtomatizacije, so lahko manj temeljite, saj avtomatizirana orodja ne kumulirajo tolikšnega znanja, niti nimajo kapacitet, ki bi zagotovile, da ne bo spregledan oziroma napačno razvrščen noben dokaz. Če avtomatizirano forenzično orodje ne da rezultata, to torej ne pomeni nujno, da dokaza ni; s tem pa je pod vprašajem zanesljivost celotne preiskave v konkretnem primeru – če preiskovalci dokazov ne iščejo sami, ne morejo vedeti, ali je bil kakšen dokaz spregledan;

— pretirano zanašanje na avtomatizirana forenzična orodja lahko prinese upadanje strokovnega znanja ter posledično zatre digitalno forenzično stroko in njen razvoj;

— sporna je predvsem avtomatizacija višjih ravni forenzičnega procesa (denimo faze analiziranja), v kateri lahko zaradi morebitnih napačnih zaključkov računalniškega progama pride do hudih napak v kazenskem postopku.

Zanesljivost in verodostojnost digitalnih forenzičnih preiskav oziroma analiz sta torej bistveni, zato kakršni koli poenostavljeni modeli na tem področju niso sprejemljivi. Vendar pa uvajanje avtomatizacije v digitalne forenzične preiskave kljub temu ni enoznačno in ima tudi določene prednosti.

Avtomatizacija omogoča ponovljivost in primerljivost rezultatov ter poenotene forenzične postopke (standardizacijo) vsaj na ravni posamezne organizacije. Nadalje so preiskave z uporabo teh orodij hitrejše, preiskovalci pa so manj obremenjeni in imajo – vsaj teoretično – več časa za izobraževanje in usposabljanje (James in Gladyshev, 2013).

2.2 Kratko o strojnem učenju in umetni inteligenci v digitalni forenziki

Kot rečeno, je avtomatizacija v digitalni forenziki trenutno najbolj široko uporabljana v uvodnih fazah digitalnega forenzičnega procesa, kjer se triaža uporablja za izločitev nerelevantnih podatkov, da ostane za poglobljeno preiskavo oziroma ročni pregled kolikor toliko obvladljiva količina podatkov. Na obzorju je tudi že naslednja faza avtomatizacije, to je inteligentna uporaba, ki presega le eliminiranje naprav in oženje kroga podatkov, ampak se razvijajo računalniški programi za vsebinsko povezovanje, razvrščanje in analiziranje podatkov (James in Gladyshev, 2013). V novejši literaturi (Iqbal in Alharbi, 2019) se kot možna rešitev z velikim potencialom za pomoč pri digitalnih forenzičnih preiskavah navaja nadgradnja avtomatizacije s strojnim učenjem, ki se pogosto povezuje tudi z umetno inteligenco. Kot opozarja Dixon (2020), se ta pojma pogosto uporabljata kot sopomenki, čeprav to nista. Strojno učenje je tehnika, ki pomaga povezovati in obdelovati velike količine podatkov in se ob tem kaj novega naučiti; umetna inteligenca pa je bistveno širši pojem ter vključuje področja računalniškega vida, robotike in obdelave naravnega jezika, pa tudi druge pristope, ki ne vključujejo tehnologij strojnega učenja (Varga, 2018). Orodja umetne inteligence lahko opravljajo človeška dela in komunicirajo z okoljem, ultimativni cilj umetne inteligence pa je razviti stroje, ki bodo delovali kot ljudje (Iqbal in Alharbi, 2019). Umetna inteligenca je torej oznaka za rešitve, ki naredijo stroje pametne (te rešitve so še zelo osnovne oziroma v povojih), strojno učenje pa je tehnologija oziroma veda o vzorcih učenja in predvidevanju rezultatov iz velikih nizov podatkov, ki je v praksi široko uporabljana na različnih področjih. Rezultati strojnega učenja se lahko zdijo »inteligentni«, gre pa v samem bistvu za rabo statističnih metod v povezavi z zmogljivo strojno in programsko opremo, ki lahko hitro obdela veliko podatkov (Varga, 2018). Sistemi strojnega učenja so se torej sposobni učiti sami na podlagi izkušenj in preteklih primerov, pri čemer se za razliko od sistemov umetne inteligence učijo iz podatkov in ne na podlagi vgrajenega programiranja (Iqbal in Alharbi, 2019).

V kriminologiji je fenomen strojnega učenja in umetne inteligence preučevan zlasti v povezavi z napovednimi algoritmi oziroma računalniškimi programi, ki izdelujejo verjetnostna poročila o prihodnji kriminaliteti, ocenjujejo verjetnost povratništva in celo predvidevajo sodne odločitve (Završnik, 2017, 2020). Ti sistemi prihodnje obnašanje napovedujejo na podlagi zgodovinske perspektive, iz katere se učijo, osnova njihovega delovanja pa je programje za prepoznavo vzorcev (Iqbal in Alharbi, 2019). Da se sistem v procesu strojnega učenja pravilno (na)uči, so potrebni reprezentativni podatki, ki vsebujejo vzorce in rezultate, s katerimi bo sistem za obdelavo podatkov delal tudi v prihodnje, hkrati pa nimajo nepomembnih informacij, ki bi lahko (z)motile proces učenja. Vsi podatki, ki se uporabijo za učenje algoritma, morajo biti ustrezno označeni in opremljeni s funkcijami, ki se ujemajo z vprašanji, ki bodo postavljena sistemu strojnega učenja (Varga, 2018). Pri tem je treba upoštevati, da so lahko pretekle odločitve oziroma podatki, na katerih temelji strojno učenje, tudi napačni ali pa temeljijo na (zavestnih ali nezavednih) predsodkih oziroma so pristranski. Če se program uči iz teh odločitev oziroma podatkov, bodo tudi njegove odločitve temu primerne, se pravi pristranske. Zagotoviti, da računalniški program pri učenju ne bo upošteval napak, predsodkov in pristranskih odločitev, ampak jih bo eliminiral, pa je silno zahtevno (Bench-Capon, 2020). Kot poudarja Varga (2018), se je v praksi precej pogosto izkazalo, da strojno učenje poveča pristranskost. Moč, a tudi šibkost sistemov strojnega učenja se torej kaže v tem, da program naredi točno (in samo) tisto, za kar je programiran[13] (Dixon, 2020).

Na področju digitalne forenzike napovedovanje prihodnjega vedenja ni pomembno, saj se digitalna forenzična preiskava osredotoča na pretekle dogodke (izvedeno kaznivo dejanje), kar pa ne pomeni, da inteligentna programska orodja ne morejo biti koristna. Garfinkel (2010) je že pred desetletjem napovedal, da bodo morali biti novi napredni sistemi sposobni filtrirati forenzične informacije na podoben način, kot to počnejo forenzični analitiki, se pravi, da je nujen razvoj programov, ki bodo sposobni zaznati in izpostaviti podatkovne elemente, ki izstopajo v konkretnem primeru. Danes so na principih strojnega učenja že razviti (in se še razvijajo in nadgrajujejo) avtomatizirani modeli, ki so sposobni iz kopice naprav izluščiti tiste z relevantnimi podatki, in nato med temi podatki izpostaviti tiste, ki so potrebni podrobnejšega pregleda, iz tehnične literature pa izhaja, da se na laboratorijski ravni na principih umetne inteligence razvijajo in preverjajo tudi modeli za avtomatizirano vsebinsko analizo podatkov (Homem, 2018; Mohammed, Clarke in Li, 2016). Iqbal in Alharbi (2019) denimo napovedujeta razvoj inteligentnih metod oziroma na strojnem učenju temelječih digitalnih forenzičnih orodij, ki bodo lahko izvajala metaanalize na podlagi metaznanja iz različnih virov in tako poenostavila

[13] Dober algoritem za prepoznavo obrazov bo denimo dal zanesljive rezultate glede primerjave obrazov, ne zmore pa nobene druge naloge (Geradts, 2018), npr. profiliranja posameznika, ki ga je prepoznal.

kompleksna forenzična opravila ter preiskovalcem ponudila razumljive in obvladljive podatkovne formate v kratkem času.

Čeprav so (če so) trenutno avtomatizirane le uvodne faze digitalnih forenzičnih preiskav in so za izvedbo kognitivno napornih in časovno zahtevnih procesov identifikacije relevantnih artefaktov oziroma dokazov še vedno odgovorni digitalni forenzični preiskovalci (Al Fahdi, Clarke, Li in Furnell, 2016), ima tehnološki razvoj na področju strojnega učenja in umetne inteligence torej potencial tudi v digitalni forenziki. Bo pa treba zaradi uporabe izsledkov forenzične preiskave v kazenskih postopkih ustrezno pozornost nameniti transparentnosti delovanja na avtomatizaciji ter umetni inteligenci temelječih forenzičnih orodij in zanesljivosti njihovih rezultatov, o čemer sledi razprava v nadaljevanju.

3 Kazenskopravni vidiki uvajanja avtomatizacije in drugih novosti v digitalne forenzične preiskave

Med temeljnimi in najpomembnejšimi načeli kazenskega procesnega prava in postopka je načelo iskanja resnice. To načelo izrecno zavezuje sodišče in državne organe, ki sodelujejo v kazenskem postopku (torej policijo in državno tožilstvo), da morajo po resnici in popolnoma ugotoviti dejstva, pomembna za izdajo zakonite odločbe, pri čemer morajo enako pazljivo preizkusiti in ugotoviti tako dejstva, ki obdolženca obremenjujejo, kakor tudi dejstva, ki so mu v korist (Šugman Stubbs, Gorkič in Fišer, 2020). Kazenski postopek je *ex post* reakcija na že izvršeno ravnanje, zato je izjemnega pomena, da se v njem ugotovi prava, objektivna resnica o preteklem dogodku, saj to omogoča pravično končno sodbo. Načelo pravičnosti kot vrhovno pravno načelo med drugim torej zahteva, da so preiskovalne metode, uporabljene v konkretnem primeru, preizkušene in zanesljive. S tega vidika uvajanje avtomatizacije v digitalne forenzične preiskave sproža naslednja (medsebojno povezana) vprašanja:

— vprašanje zanesljivosti avtomatiziranih digitalnih forenzičnih (pod)procesov,
— vprašanje zanesljivosti avtomatiziranih digitalnih forenzičnih orodij in
— vprašanje vsebinske celovitosti oziroma zanesljivosti (delno) avtomatizirano pridobljenih digitalnih dokazov.

Osrednji izziv pri prepuščanju dela preiskovalnih dejavnosti računalniškemu programu (algoritmu) je torej zagotavljanje zanesljivosti izsledkov, kar je zelo pomembno v vseh pravnih postopkih, absolutno bistveno pa v kazenskem postopku, kjer lahko pravična (oprostilna ali obsodilna) sodba temelji le na objektivno in celovito ugotovljenem dejanskem stanju. Pogoj za pravilno uporabo prava so torej pravilno razrešena dejanska vprašanja, kar predpostavlja, da je zakonito ugotovljen obstoj vseh tistih pravno pomembnih dejstev, na katera vežeta kazensko materialno in procesno pravo svoje posledice (Dežman, 2013).

3.1 Zanesljivost digitalnih forenzičnih procesov – koristnost standardizacije

Ker je digitalna forenzika sorazmerno mlada disciplina, ni pretirane konsistence med industrijo (razvijalci forenzičnih programskih orodij) in sodno prakso, in tudi ne standardiziranih forenzičnih procesov, orodij in izobraževanj (Lopez et al., 2016). Univerzalno sprejeta standardizacija postopkov in ravnanja z digitalnimi dokazi bi bila s pravnega vidika zelo dobrodošla, saj bi zagotavljala določeno mero sistemske zanesljivosti izsledkov digitalnih forenzičnih preiskav (digitalna forenzika je v osnovi tehnična znanost). Premiki na tem področju so, vendar razmeroma počasni. V zadnjem desetletju so se sprejeli ISO standardi,[14] ki vsebujejo seznam priporočil za izvajanje digitalnih forenzičnih preiskav in za ravnanje z digitalnimi dokazi, vendar v nobeni državi nimajo statusa pravno predpisanih oziroma obvezujočih standardov na način, da bi lahko digitalne forenzične preiskave za potrebe kazenskih (in drugih sodnih) postopkov izvajale le organizacije, ki so pridobile ustrezen ISO certifikat. Poleg tega strokovnjaki iz prakse opozarjajo, da ima ISO 27037/2012, ki je prvi seznam priporočil za identifikacijo, zbiranje, pridobivanje in ohranitev digitalnih dokazov, ki je uradno priznan na mednarodni ravni, določene pomanjkljivosti, zaradi katerih je primeren le kot izhodišče, ne bi pa smel biti izključna osnova za ravnanje z digitalnimi dokazi. Kot v drugih podobnih primerih gre za živ standard, ki ga je treba prilagajati okoliščinam konkretnega primera na način, da ne pride do konflikta med zahtevami standarda in prakso (Veber in Smutny, 2015). Smernice, priporočila, mnenja in druge dokumente za ravnanje z digitalnimi dokazi izdajajo tudi znanstvena delovna skupina za digitalne dokaze – *Scientific Working Group on Digital Evidence*

[14] Konkretno:
– ISO 27037:2012 – Smernice za identifikacijo, zbiranje, pridobivanje in ohranitev
– digitalnih dokazov (*Guidelines for identification, collection, acquisition, and preservation of digital evidence*),
– ISO/IEC 27041:2015 – Smernice za zagotavljanje primernosti in ustreznosti metode preiskave incidentov (*Guidance on assuring suitability and adequacy of incident investigative method*),
– ISO 27042:2015 – Smernice za analizo in interpretacijo digitalnih dokazov (*Guidelines for the Analysis and Interpretation of Digital Evidence*) in
– ISO/IEC 27043:2015 – Načela in postopki za preiskovanje incidentov (*Incident Investigation Principles and Processes)*.

(SWGDE), mednarodne organizacije (npr. Svet Evrope, 2020), organi Evropske unije (npr. Evropska agencija za kibernetsko varnost, 2015) in Evropska mreža inštitutov za forenzične znanosti (European Network for Forensic Science Institutes [ENFSI], 2015), na voljo pa so tudi številni forenzični priročniki, ki so jih pripravili strokovnjaki iz teorije in iz organov, ki opravljajo preiskave v praksi, vendar nič od navedenega ne predstavlja pravno veljavnih in zavezujočih standardov na nacionalni ali nadnacionalni ravni. Ob odsotnosti univerzalnih pravil oziroma standardov za izvajanje digitalnih forenzičnih procesov digitalni forenziki preiskave tako opravljajo predvsem na podlagi svojih izkušenj in politike svoje organizacije (Iqbal in Alharbi, 2019), kar lahko na globalni, pa tudi na regionalni in v večjih državah celo nacionalni ravni ustvarja precejšnjo neenakost pri izkoriščanju potenciala digitalne forenzike v kazenskih postopkih.

3.2 Zanesljivost digitalnih forenzičnih orodij – potreba po validaciji in merjenju natančnosti

O potrebni validaciji in verifikaciji digitalnih forenzičnih programskih orodij in certificiranju digitalnih forenzičnih preiskovalcev se razpravlja že dlje časa, vendar sistemskih premikov na globalni ravni[15] na tem področju ni (Caviglione et al., 2017). Predpisan model validacije in verifikacije posameznega digitalnega forenzičnega orodja bi imel pozitivne učinke na področju zaupanja v rezultate digitalnih forenzičnih preiskav ter bi olajšal tudi uvajanje avtomatizacije in drugih novosti v digitalne forenzične preiskave. Evropska unija na določenih področjih[16] zaradi harmonizacije pravil določa, da morajo proizvajalci določene opreme poskrbeti za validacijo te opreme, njeni uporabniki pa so zadolženi za njeno verifikacijo, v okviru katere se običajno opravi vsaj merjenje stopnje napak oziroma ocena netočnosti.[17] Na področju digitalne forenzike česa podobnega v kratkem verjetno ni mogoče pričakovati. Zaradi izjemne raznolikosti elektronskih naprav in formatov podatkov ter stalno porajajočih se novih digitalnih svetov (družbena, omrežja, storitve v oblaku, IoT[18]) sta validacija in verifikacija digitalnih forenzičnih orodij s testiranjem[19] po klasičnih postopkih na meji mogočega. To seveda ne pomeni, da se ta orodja ne testirajo; je pa realnost taka, da so ta testiranja pogosto opravljena le formalno in na hitro (površno), čemur botrujejo komercialni razlogi (tj. prehiteti druge podobne izdelke, ki vstopajo na trg, ali biti prvi pri lansiranju na novo nastajajoče tehnologije na trg), pa tudi veliki stroški, velik vložek časa in usposobljenih kadrov ter odsotnost preverljivega in rekurzivnega protokola za testiranje (Arshad, Bin Jantan in Oludare, 2018). Tudi dobre prakse, kakršen je program za testiranje računalniških forenzičnih orodij (*Computer Forensics Tool Testing Program,* [CFTT]), ki ga izvaja Ameriški nacionalni institut za standardizacijo in tehnologijo (*The National Institute of Standards and Technology,* [NIST]), imajo svoje omejitve. NIST-ovo testiranje CFT temelji na znanstvenih metodah, rezultate pa preverita obe strani (proizvajalec in organizacija, ki izvede testiranje), kar zagotavlja določeno stopnjo poštenosti. Težava je v tem, da so ta testiranja dolgotrajna in je v času objave rezultatov pogosto na trgu že naslednja (ponovno neodvisno netestirana) različica digitalnega forenzičnega orodja (Flandrin, Buchanan, Macfarlane, Ramsay in Smales, 2014).

Kot izhaja iz literature, se v praksi forenzični preiskovalci pogosto (pretirano) zanašajo kar na evalvacijo, ki jo je za lastno digitalno forenzično orodje opravil proizvajalec tega orodja (Flandrin et al., 2014), oziroma preprosto predpostavljajo, da forenzično orodje, ki ga uporabljajo, dela in zmore točno to, kar trdi njegov proizvajalec oziroma prodajalec (Dimpe in Kogeda, 2019), tudi če za to ni posebnih zagotovil. Smernice ENFSI (2015) poudarjajo, da bi moral forenzični laboratorij oziroma institucija, ki opravlja digitalne forenzične preiskave, načeloma dati prednost digitalnim forenzičnim orodjem, ki so funkcionalno verificirana ali vsaj v čim večji meri preizkušena oziroma testirana s strani neodvisnih institucij, vendar pa tega pogosto ni mogoče zagotoviti. Kot rečeno, splošne metodologije za evalvacijo vseh vrst digitalnih forenzičnih orodij v vseh možnih situacijah ni mogoče razviti. Tudi proizvajalci teh orodij, ki se resno lotijo njihovega testiranja, pri tem ne morejo predvideti vseh scenarijev, v katerih bo orodje lahko uporabno

---

[15] Posamezne države na tem področju sicer sprejemajo določena priporočila (npr. Forensic Science Regulator, 2020).

[16] Tako ureditev vsebuje na primer Direktiva 98/79/ES Evropskega parlamenta in Sveta z dne 27. oktobra 1998 o in vitro diagnostičnih medicinskih pripomočkih (1998).

[17] Dogša (1993) validacijo definira kot proces vrednotenja programske opreme na koncu njenega razvoja z namenom, da se ugotovi skladnost izdelane programske opreme z zahtevami, verifikacija pa ima več pomenov in se opredeljuje: 1) kot proces, pri katerem se preverja, ali produkt tekoče faze ustreza zahtevam, postavljenim v predhodni fazi, 2) kot formalno dokazovanje pravilnosti programov oziroma in 3) kot sinonim za vse vrste preverjanj.

[18] Internet stvari (ang. *internet of things,* IoT) je pojem, ki zajema vsakdanje naprave, povezane v internetno omrežje na način, da si izmenjujejo podatke. Po navadi se delijo v dve skupini: tiste za potrošniško rabo (pametne hiše, povezana vozila, digitalno zdravstvo) in tiste za industrijsko rabo (maloprodaja, povezane zgradbe, kmetijstvo). Nekatere od naprav IoT so čisto običajne naprave, ki so jih sčasoma nadgradili z internetno povezavo (televizije, hladilniki), medtem ko so druge senzorične ali sprožilne naprave, ki so bile razvite kot vrsta IoT (Lillis et al., 2016).

[19] Testiranje je analiza programa (ali samo komponente), ki se izvaja z namenom preverjanja, ali program ustreza zahtevam oziroma da se pokaže razlika med pričakovanimi in dejanskimi izhodnimi vrednostmi (Dogša, 1993).

(Flandrin et al., 2014), zato se nekateri avtorji zavzemajo za model, skladno s katerim naj evalvacijo posameznega digitalnega forenzičnega orodja pred začetkom njegove uporabe opravijo digitalni forenzični preiskovalci sami, lahko tudi ob upoštevanju scenarija oziroma okoliščin konkretnega primera (Bhatt, AlZahrani in Wani, 2021).

Vendar pa tudi to ni preprosto. Večina preiskovalcev uporablja komercialna digitalna forenzična orodja, katerih natančni način delovanja ni znan, ker proizvajalci niso naklonjeni razkritju programskih kod (Vincze, 2016).[20] Posledično lahko verifikacija teh orodij (*ad hoc* ali sistemska) poteka le v obliki t. i. *black-box* testiranja (tj. po načinu črne skrinjice), ki zajema preverbo delovanja digitalnega forenzičnega orodja brez dostopa do izvorne kode, se pravi brez vpogleda v notranjo strukturo oziroma delovanje programa. V okviru te verifikacije je tudi z vidika uvajanja avtomatizacije v digitalne forenzične preiskave – teoretično gledano – zelo pomembno preverjanje natančnosti (zanesljivosti) uporabljenih forenzičnih orodij. Vendar je tudi merjenje stopnje napak (ang. *error rate*), ki je v znanosti sicer zelo pomembno za ugotavljanje zanesljivosti določene metode, na področju digitalne forenzike specifično. Stopnja napak se meri kot pogostost napak pri določeni metodi, pri čemer se iščejo lažno pozitivni in lažno negativni zadetki. S to metodo se praviloma iščejo naključne napake, ki izvirajo iz neznane in nepredvidljive spremembe med poskusom. Težava pri digitalnih forenzičnih tehnikah oziroma orodjih je, da je večina napak sistematičnih (programskih) in ne naključnih, zato s standardiziranimi postopki ugotavljanja stopnje napak ni mogoče potrditi zanesljivosti in točnosti teh programov oziroma orodij. Nadalje se za vsak zanesljiv statistični izračun predpostavlja, da bistvene sestavine ostajajo statične (npr. kri za analizo DNK); digitalna infrastruktura pa je izjemno dinamična in se nenehno pojavljajo nove vrste medijev in naprav (npr. Facebook, podatki v oblaku, pogon SSD), ki se popolnoma razlikujejo od starejših medijev in naprav. Posledično se orodje oziroma metoda, ki je bila z visoko natančnostjo preizkušena na primer na eni vrsti trdega diska, lahko izkaže za popolnoma netočno pri drugi vrsti diska (Arshad et al., 2018).

Z vidika zanesljivosti digitalnih forenzičnih orodij je pomenljiv tudi podatek, da niti najpogosteje uporabljena oziroma komercialno najbolj razširjena digitalna forenzična orodja niso testirana z vidika antiforenzičnih napadov. Bhatt et al. (2021) so opravili preizkus, ki je vključeval štiri orodja (Sleuth Kit, EnCase, FTK in OSForensics) in enajst različnih antiforenzičnih napadov. Študija je pokazala, da so vsa štiri orodja uspešno zaznala le tri napade (skrivanje podatkov, skrivanje podatkovne montaže in enkripcijo), medtem ko kar štirih napadov ni zaznalo nobeno orodje (varno brisanje podatkov, brisanje sledi s ponarejanjem časovnega žiga, brisanje sledi s spremembo datotečnega podpisa in prisotnost stisnjene bombe, ki lahko v primeru, če jo odprejo, prepiše relevantne digitalne podatke oziroma uniči dokaze). Ostale štiri napade so nekatera orodja zaznala, druga pa ne. Avtorji zaključujejo, da izpostavljene ranljivosti digitalnih forenzičnih orodij postavljajo pod vprašaj njihovo kredibilnost. To je eno od vprašanj, ki bi moralo biti razrešeno v procesu validacije in verifikacije teh orodij; v odsotnosti pa gre za okoliščino, o kateri mora v konkretnem primeru na koncu odločiti sodišče, ko odloča o (ne)sprejemljivosti določenega digitalnega dokaza.

Čeprav so temelji digitalne forenzike (računalniška znanost, fizika, elektronika) razmeroma trdni in v osnovi podprti z matematično znanostjo (ENFSI, 2015), je njeno delovno področje – ob upoštevanju hitrega razvoja tehnologije in s tem povezane podatkovne ekspanzije – očitno torej preveč dinamično, da bi se (že) lahko ustalila kot splošno priznana znanstvena disciplina s trdnimi teoretičnimi in metodološkimi temelji. Kot rečeno, to pred posebne izzive postavlja pravosodne organe kot osrednje uporabnike njenih storitev. Uporaba znanstveno nepreizkušenih tehnik za dokazovanje v kazenskem postopku je inherentno problematična, zato digitalni dokazi pogosto le s težavo zadostijo strogim znanstvenim kriterijem, ki načeloma veljajo za izvedenska dela v kazenskih postopkih (Arshad et al., 2018).

3.3 Zanesljivost digitalnih dokazov

Forenzični priročniki in standardi večinoma molčijo o konceptu »veljavnega digitalnega dokaza« oziroma ne vzpostavljajo procedure za validacijo digitalnih dokazov (Shanmugam, Powell in Owens, 2011). Tudi na pravnem področju posebnih postopkov za validacijo teh dokazov ni, ampak veljajo enaka pravila kot za vse druge dokaze. Da je digitalni dokaz uporaben na sodišču, mora izpolnjevati dva osnovna pogoja: biti mora pravno dopusten in imeti mora ustrezno dokazno vrednost (Selinšek, 2010). Pravna dopustnost se presoja z vidika ustavnih in zakonskih standardov, določenih za postopanje z dokazi. Le če je vir spoznanja o kakšnem pravno pomembnem dejstvu pridobljen na zakonit način, lahko postane dokaz v kazenskem postopku. Dokazi, pridobljeni na pravno nedovoljen način (to je s kršitvijo ustavno določenih pravic in temeljnih svoboščin ali s kršitvijo nekaterih določb kazenskega postopka ter dokazi, pridobljeni na podlagi nedovoljenega dokaza), so predmet izločitve (Dežman, 2013). Kar se tiče dokazne vrednosti digitalnih dokazov, velja načelo proste presoje dokazov, pri čemer teorija izpostavlja, da je treba pri presoji upoštevati tudi naravo oziroma značilnosti digi-

[20] Varga (2018) opozarja, da so modeli »črne skrinjice« pravilo tudi pri sistemih strojnega učenja, kar je v praksi sicer lahko učinkovito, a bi bilo bistveno bolje, če bi uporabniki imeli vpogled v to, na podlagi katerih vzorcev so se algoritmi kaj naučili, in s tem možnost odločanja, ali njihovemu rezultatu verjamejo ali ne.

talnih dokazov in v tem okviru predvsem naslednje elemente (Selinšek, 2011):

— avtentičnost (vsebinska verodostojnost, vključno z izkazano vzročno zvezo med dokazom in domnevnim storilcem kaznivega dejanja in med dokazom in elektronsko napravo, v kateri je shranjen);
— neokrnjenost oziroma integriteto (dokaz, predočen sodišču, mora biti popolnoma enak (nespremenjen), kot je obstajal ali nastal v času storitve kaznivega dejanja[21]);
— preverljivost (ključno je izvajanje preiskave na identični kopiji nosilca dokaza in pravilno dokumentiranje dela v obliki skrbniške verige);
— vsebinsko celovitost (dokaz je treba ovrednotiti samostojno in tudi v povezavi z drugimi dokazi v tem primeru) in
— zanesljivost (način pridobitve dokaza in ravnanje z njim ne smeta vzbujati dvoma o avtentičnosti in verodostojnosti dokaza).

Horsman (2020) v razpravi o nujno potrebni reviziji in nadgradnji ACPO načel dobre prakse za digitalne dokaze (*ACPO Good Practice Guides for Digital Evidence*)[22] med drugim predlaga sprejetje novega načela, skladno s katerim bi bili vsi z digitalno forenzično preiskavo izluščeni podatki, ki naj postanejo digitalni dokazi, podvrženi testu, s katerim bi se z uporabo splošno sprejetih testnih metod preverila njihova točnost oziroma zanesljivost. Taka (čim bolj univerzalno odobrena) metodologija bi na sistemski ravni dvignila raven kakovosti in zanesljivosti digitalnih forenzičnih preiskav ter sodiščem omogočila, da se pri odločanju in obrazložitvi odločitve naslonijo na argument »akreditiranega« dokaza.

Sodna praksa v ZDA je za ločevanje prave oziroma zanesljive znanosti od »smetiščne« (ang. *junk*) znanosti oblikovala t. i. Daubertov test,[23] skladno s katerim sodišče v primeru potrebe po ocenjevanju zanesljivosti izvedenskega mnenja s področja digitalne forenzike oziroma verodostojnosti digitalnih dokazov presoja naslednje (DeMatteo, Fishel in Tansey, 2019):

— ali je uporabljena znanstvena metoda za izvedbo digitalne forenzične preiskave že testirana oziroma ali obstaja empirični dokaz o njeni zanesljivosti;
— ali je bila metoda predmet medsebojnega strokovnega pregleda (ang. *peer-review*) in objavljena v znanstveni literaturi;
— ali je na voljo zanesljiva ali vsaj verjetnostna stopnja napak, ki jih generira uporaba te metode, in
— ali je uporabljena metoda oziroma postopek splošno sprejet v digitalni forenzični skupnosti.

Čeprav morajo digitalne forenzične preiskave primarno zadostiti pravnim standardom države, v kateri se izvajajo, je Daubertov test v literaturi s področja digitalne forenzike citiran po vsem svetu (Flandrin et al., 2014). Navedeni kriteriji so sodnikom lahko v pomoč, kadar se v kazenskem postopku pojavijo dvomi v zvezi s postopkom pridobitve določenega digitalnega dokaza, vendar stroka poudarja, da niso izključujoči. Tudi če je odgovor na vsa vprašanja negativen, to nujno ne pomeni, da dokaz na sodišču ni uporaben. Če ga potrjujejo druge okoliščine primera (npr. priče), ga sodišče še vedno lahko šteje za verodostojnega in dokazno vrednega (Arshad et al., 2018). Tudi v našem pravnem redu načelo proste presoje dokazov, tesno povezano z načelom iskanja resnice, sodišču in državnim organom, ki sodelujejo v kazenskem postopku, zagotavlja, da njihova presoja, ali je podano kakšno dejstvo ali ne, ni vezana na nobena posebna formalna dokazna pravila in tudi ne z njimi omejena. Presoja dokaznega gradiva v kazenskem postopku temelji na t. i. psihološki dokazni oceni, ki ni vnaprej usmerjana z zakonskimi dokaznimi pravili, pa tudi ne arbitrarna. Sodišče mora vestno pretehtati vsak pravno dopusten dokaz posebej ter v zvezi z drugimi dokazi in na podlagi take presoje sprejeti sklep, ali je kakšno dejstvo dokazano ali ne (Selinšek, 2020; Šugman Stubbs et al., 2020). To (načeloma enostavno) pravilo lahko postane v primeru dvoma v izsledke digitalne forenzične preiskave precej zahtevno. Sodnik sam praviloma nima znanj s področja izvajanja digitalnih forenzičnih preiskav, ki bi mu omogočila neposredno vsebinsko presojo, ali je izražen dvom upravičen ali ne. Preden v postopek pritegne novega izvedenca (ali celo izvedence) ali pa potem, ko že ima več različnih mnenj o istem vprašanju, je smiselno, da sodišče preveri način oziroma metodo, s katero je bil sporni digitalni dokaz pridobljen (tudi ob upoštevanju kriterijev iz Daubertovega testa, ki so univerzalne narave). Pri tem je zelo pomembna vloga digitalnega forenzičnega preiskovalca, ki mora biti za potrebe sodnega odločanja sposoben razložiti, kako je bil digitalni dokaz pridobljen, ohranjen in analiziran (Bryce, McDougle in Robertson, 2017), sodnik pa mora znati od njega to zahtevati. Tako bo lahko tudi v primeru, ko ima v

[21] Shanmugam et al. (2011) predlagajo model, v katerem bi se integriteta posameznega digitalnega dokaza preizkusila z antiforenzičnim pristopom na način, da bi se pri pridobivanju digitalnega dokaza v vsaki fazi forenzičnega procesa preverjala morebitna prisotnost antiforenzičnih aktivnosti v zvezi s tem dokazom.

[22] Gre za priročnik, ki ga je izdalo takratno britansko združenje policijskih načelnikov (*Association of Chief Police Officer's*) leta 1998, zadnjič pa je bil revidiran leta 2012. Načela so presegla veljavnost zgolj za članice tega združenja (ki se je leta 2015 sicer preoblikovalo v Nacionalni svet načelnikov policije), ampak jih povzemajo tudi številne druge organizacije, kot sta Interpol in ENISA. Dokument vsebuje štiri načela (prepoved vsakršnega spreminjanja podatkov, restriktivnost pri dostopu do izvirnih podatkov, obveznost revizijske sledi in ponovljivost forenzičnih postopkov ter odgovornost vodje preiskave), ki so še vedno aktualna, bi pa potrebovala ustrezno nadgradnjo (Horsman, 2020).

[23] Metoda je dobila ime po sodbi v zadevi Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).

končni fazi dve ali več različnih (izvedenskih) mnenj o istem vprašanju, odloči, katero je pravilno oziroma verodostojno. Če to ni mogoče in glede konkretnega digitalnega dokaza še vedno o(b)stajajo nejasnosti, je v kazenskem postopku treba uporabiti pravilo, skladno s katerim se v dvomu odloči v korist obdolženca (*in dubio pro reo*). Morebitne nasprotujoče si trditve digitalnih forenzičnih strokovnjakov[24] torej dajejo obrambi v kazenskih postopkih razmeroma široke možnosti za izpodbijanje digitalnih dokazov in lahko – ob upoštevanju vzpostavljenih pravnih standardov dokazovanja in načela poštenega postopka – tudi onemogočajo uporabo oziroma upoštevanje digitalnega dokaza v konkretnem primeru.

Standardizacija postopkov na področju digitalne forenzike ter validacija in verifikacija digitalnih forenzičnih orodij tako ni le tehnično vprašanje, ampak je pomembna tudi s pravnega vidika. Če je digitalna forenzična preiskava izpeljana skladno s sprejetimi standardi in z ustrezno validiranim in verificiranim digitalnim forenzičnim orodjem, se možnost izražanja dvoma o njenih rezultatih v kazenskem (ali drugem pravnem) postopku pomembno zmanjša.

3.4 Paradoks avtomatizacije in vloga digitalnih forenzikov

V nadaljevanju se glede na vse povedano osredotočamo na avtomatizacijo digitalnih forenzičnih preiskav. Prepuščanje (čeprav le uvodnega) dela preiskovalnih opravil računalniškim algoritmom s preiskovalnega in pravnega vidika predvsem sproža vprašanje, ali je mogoče zagotoviti, da med »avtomatično« obdelanimi (in izločenimi) podatki ne bo spregledan kakšen vsebinsko relevanten digitalni dokaz in s tem prizadeto oziroma kršeno načelo iskanja resnice. Ali je torej (delno) avtomatizirana digitalna forenzična preiskava kot celota lahko vsebinsko verodostojna do te mere, da je vsak digitalni dokaz, pridobljen v tej preiskavi, dokazno polnovreden, hkrati pa ima veljavno dokazno sporočilnost tudi dejstvo, da med preiskavo določen dokaz ni bil najden.

V zvezi s tem je treba izpostaviti, da je v pravu bistvena obrazložitev oziroma argumentacija, algoritmi pa sprejete odločitve ne obrazložijo oziroma je ta obrazložitev tehnična in ne vsebinska (Bench-Capon, 2020). Dejstvo, da proizvajalci digitalnih forenzičnih orodij ne želijo razkriti izvorne kode teh orodij, ne otežuje le testiranja teh orodij, ampak je tovrstna zadržanost problematična tudi s pravnega vidika. Dixon (2020) meni, da bi transparentnost na tem področju povečala zaupanje v avtomatizirana forenzična orodja, saj dejstvo, da razvijalec določenega orodja ne želi razkriti načina notranjega delovanja svojega produkta ali celo ne zna pojasniti, kako je program prišel do določene rešitve, vzbuja nezaupanje v to orodje. Kot pojasnjeno, se to nezaupanje v kazenskem postopku lahko odrazi v obliki nižje (slabše) dokazne vrednosti ali celo odklonitvi določenega digitalnega dokaza na sodišču.

Podrobnejši premislek glede transparentnosti bi terjal poznavanje razlogov, zakaj razvijalci digitalnih forenzičnih orodij ne želijo razkriti izvornih programskih kod. Kot očiten se kaže razlog varovanja avtorskih pravic in s tem povezan komercialni interes podjetja, ki razvija določeno orodje. So pa mogoči tudi drugi potencialni razlogi, ki izvirajo iz samega delovanja programa (tudi ti na koncu sicer spet sovpadejo s komercialnim interesom). Denimo, da bi – zelo poenostavljeno – transparentno razkrita koda (delno) avtomatiziranega digitalnega forenzičnega orodja brez dvoma pokazala, da bo to orodje v fazi avtomatiziranega delovanja našlo 80 % relevantnih dokazov, 20 % pa jih bo spregledalo. Ali si lahko kateri koli pravosodni sistem na svetu, ki temelji na načelih iskanja resnice in poštenega sojenja, privošči dokazovanje na podlagi uporabe takega orodja? Na načelni ravni se seveda zdi, da je odgovor odločno negativen. Vendar pa velja biti previden in se nadalje vprašati, ali obstajajo zagotovila, da ne prihaja do spregleda ali napačnega vrednotenja dokazov tudi pri klasičnih (»ročnih«) digitalnih forenzičnih preiskavah, vključno s primerjavo te možnosti pri drugih vrstah preiskav (npr. pri hišni preiskavi ali bioloških, fizikalnih, daktiloskopskih, kemijskih in drugih forenzičnih preiskavah).

Tehnično gledano, skoraj zagotovo ni in ne bo mogoče doseči, da pri digitalni forenzični preiskavi ne bo spregledan nobeden (obremenilni ali razbremenilni) dokaz. Toda tudi brez empiričnih raziskav je mogoče enako trditi za »ročne« preiskave oziroma preiskovalce. Pomanjkanje znanja in izkušenj lahko vodi k spregledu ključnih dokazov in napačnim zaključkom, kar se dogaja tudi brez uporabe avtomatiziranih orodij. Kot ugotavljata James in Gladyshev (2013), **če** se izkušeni preiskovalci pretirano zanašajo na avtomatizacijo, lahko pride do stagnacije digitalne forenzične profesije, po drugi strani pa lahko slabo usposobljenim ali neizkušenim preiskovalcem avtomatizirano orodje omogoči, da bodo našli in ovrednotili dokaze, ki bi jih sicer spregledali. Ker čas, denar in pravica vedno tekmujejo, so mnogi preiskovalci naučeni, da v začetni fazi zaženejo avtomatizirano forenzično orodje, nato pa ročno analizirajo rezultate. Tudi če domnevamo (zaupamo), da je avtomatizacija, vgrajena v določeno forenzično orodje, zanesljiva, sta torej še vedno bistveni zanesljivost preiskovalca, da je pravilno uporabil avtomatizirano forenzično

[24] Casey (2019) navaja primer, ko prvi digitalni forenzik, ki je pripravil mnenje v kazenskem postopku, brez dvoma zaupa rezultatom avtomatiziranih operacij za obnovitev datotek in zaključi, da je bila nerazdeljena datoteka v konkretnem primeru »popolnoma obnovljena«. Ko je v postopek pritegnjen še drugi digitalni forenzik, pa izrazi dvom o zanesljivosti avtomatiziranih sistemov za obnovitev datotek in glede datoteke v konkretnem primeru ne izpelje jasnega zaključka.

orodje, in njegova sposobnost, da pravilno interpretira dobljene rezultate (James in Gladyshev, 2013).

Avtomatizacija v digitalni forenziki torej sproža svojevrsten paradoks, ki ga Borhaug (2019) definira tako: »Bolj, kot je avtomatiziran sistem učinkovit, bolj je ključen človeški nadzor. Preiskovalci so torej manj vključeni v delo, vendar je njihova vključenost bolj pomembna oziroma ključna.« Z vidika organov odkrivanja in pregona to ustvarja zahtevno dilemo: avtomatiziranje preiskovanja je nujno[25] (predvsem za zmanjšanje zaostankov), vendar več avtomatizacije povečuje možnost napačnih odločitev, če ni v enaki meri ojačana človeška kontrola. Tudi s tega vidika je bistveno, da digitalni forenzični preiskovalec razume in pozna procese, ki jih izvaja računalniški program,[26] in je (izkazano) sposoben kritično pregledati rezultate, ki jih v konkretnem primeru dobi z uporabo določenega digitalnega forenzičnega orodja (Bryce et al., 2017). S tem smo odgovorili tudi na uvodno zastavljeno vprašanje oziroma tezo: glede na trenutno sistemsko stanje na področju digitalne forenzike avtomatizirano digitalno forenzično orodje lahko *opravi* določen (uvodni) del digitalne forenzične preiskave, ne more pa *prevzeti* nobenega dela te preiskave v tem smislu, da ne bi bila potrebna človekova kontrola avtomatizirano pridobljenih podatkov.

V digitalnem forenzičnem procesu so kljub čedalje večjemu tehnološkemu napredku preiskovalci torej še vedno enako pomembni kot programska orodja. Podobno kot pri digitalnih forenzičnih orodjih tudi izobraževanje in certificiranje digitalnih forenzičnih preiskovalcev nista sistemsko urejena (niti globalno niti regionalno in tudi ne nacionalno). Digitalna forenzika je vključena v študijske programe fakultet s področja računalniških in matematičnih znanosti in tudi varstvoslovja,[27] vendar pa diploma iz tega predmeta praviloma ne zagotavlja usposobljenosti za izvajanje digitalnih forenzičnih preiskav. Določeno raven praktičnega znanja zagotavljajo izobraževalni programi za pridobitev certifikatov s področja digitalne forenzike, ki jih ponujajo nekatere zasebne institucije. Med ne-neodvisnimi je treba omeniti certifikata, ki ju izdajata oba največja proizvajalca digitalnih forenzičnih orodij: podjetje AcessData ponuja program AccessData preizkušeni preiskovalec (*AccessData Certified Examiner*), v okviru katerega se kandidati specializirajo za uporabo njihovega forenzičnega orodja Forensic Toolkit (FTK), podjetje Guidance Software pa ponuja certifikat EnCase preizkušeni preiskovalec (*EnCe: EnCase Certified Examiner*), ki potrjuje usposobljenost za ravnanje z njihovim digitalnim forenzičnim orodjem EnCase. Med neodvisnimi zasebnimi institucijami je globalno najmočnejši certifikacijski »organ« inštitut SANS iz ZDA, ki v okviru svojega programa GIAC (*Global Information Assurance Certification*) ponuja certifikata GIAC preizkušeni forenzični preiskovalec (*GIAC Certified Forensic Examiner,* [GCFE]) in GIAC preizkušeni forenzični analitik (*GIAC Certified Forensic Analyst,* [GCFA]). Priznan je tudi certifikat IACIS preizkušeni forenzični računalniški preiskovalec (*Certified Forensic Computer Examiner,* [IACIS CFCE]), ki ga je mogoče pridobiti pri mednarodnem združenju računalniških preiskovalnih specialistov (*International Association of Computer Investigative Specialists,* [IACIS]). Podobno, kot se za posamezno institucijo formalno ne zahteva, da bi morala imeti za opravljanje digitalnih forenzičnih preiskav za potrebe kazenskega postopka na primer ustrezen ISO ali drug certifikat ali akreditacijo, tudi za posameznike, ki opravljajo digitalne forenzične preiskave, niso predpisani posebni pogoji glede izobrazbe in kvalifikacij, ampak je doseganje ustrezne strokovne ravni prepuščeno posamezniku oziroma njegovemu delodajalcu. To je za tako pomemben in zahtevan poklic neprimerno. Država, ki je odgovorna do lastnega pravosodnega sistema, bi morala ob pomoči univerz premisliti o vzpostavitvi ustreznega certifikacijskega modela, na primer v obliki nacionalno regulirane temeljne kvalifikacije za digitalnega forenzičnega preiskovalca, v okviru katere bi morali imetniki kvalifikacije nato periodično (glede na hiter razvoj področja verjetno vsaj enkrat letno) obnavljati in nadgrajevati znanje ter po določenem časovnem obdobju obnoviti tudi kvalifikacijo samo.[28]

4 Sklep

Digitalna forenzika je (že po sili razmer) eno od stalno napredujočih in hitro razvijajočih se področij sodobnega časa. Nagel tehnološki razvoj zahteva hiter in stalen razvoj te di-

[25] Opuščanje avtomatizacije na drugi strani prav tako ustvarja tveganje za nepravične odločitve, saj se podaljšujejo preiskovalni zaostanki in posledično daljšajo sojenja (Borhaug, 2019).

[26] Priročnik ENFSI (2015) navaja, da forenzični analitik, ki ne razume delovanja in/ali omejitev forenzičnega orodja, ki ga je uporabil za analizo, mnenja sploh ne bi smel dati.

[27] V Sloveniji je predmet digitalna oziroma računalniška forenzika na različnih stopnjah na voljo na Fakulteti za računalništvo in informatiko Univerze v Ljubljani, na Fakulteti za matematiko in fiziko Univerze v Ljubljani, na Fakulteti za elektrotehniko, računalništvo in informatiko Univerze v Mariboru, na Fakulteti za varnostne vede Univerze v Mariboru in na Fakulteti za informacijske študije v Novem mestu.

[28] Čeprav poklica nista primerljiva, bi lahko v Sloveniji kot formalno ogrodje za ta sistem služil model nacionalno regulirane temeljne kvalifikacije za voznike motornih vozil v cestnem prometu (t. i. koda 95 za poklicne voznike), v okviru katerega je vzpostavljen program za pridobitev te kvalifikacije, program obveznega rednega usposabljanja in program za obnovitev kvalifikacije, ki velja pet let. Prim. četrto poglavje Zakona o prevozih v cestnem prometu (ZPCP-2, 2006) in Pravilnik o temeljnih kvalifikacijah za voznike motornih vozil v cestnem prometu (2010).

scipline, saj bi nasprotno ostala neizkoriščena ogromna baza potencialnih dokazov o kaznivem dejanju. Ta razvoj poteka v dveh smereh: na tehničnem oziroma programskem področju se nadgrajujejo oziroma razvijajo digitalna forenzična orodja, na pravnem področju pa se razvijajo določbe, ki postavljajo preiskovalne standarde za pridobivanje digitalnih dokazov in urejajo povezana pravna vprašanja. V mešanici obojega se iščejo možnosti za izboljšanje digitalnih forenzičnih procesov tako, da bi se v največji možni meri še lahko vsebinsko primerno obvladal ogromen obseg elektronskih podatkov oziroma potencialnih digitalnih dokazov.

V prispevku smo preverjali, kako novosti in spremembe v digitalnih forenzičnih preiskavah vplivajo na uporabnost (zanesljivost) rezultatov teh preiskav. Izbrali smo avtomatizacijo, ki v digitalni forenziki sama po sebi sicer ni novost, saj so določene dejavnosti v okviru digitalne forenzične preiskave že dolgo avtomatizirane (prevajanje iz strojnega v berljiv jezik, računanje zgoščene vrednosti), se pa ta zaradi podatkovne ekspanzije nadgrajuje in širi tudi na bolj vsebinska področja. Avtomatizirano filtriranje podatkov kot eden od odgovorov na čedalje večje količine elektronskega gradiva, ki ga je treba preiskati, je v uvodnih fazah digitalnega forenzičnega procesa že razmeroma vpeljano, avtomatiziranje višjih ravni (predvsem analize) pa je še v povojih. Avtomatizacija, temelječa tudi na strojnem učenju in umetni inteligenci, (bo) nedvomno lahko do določene mere nevtralizira(la) kompleksnost digitalnih forenzičnih preiskav (Caviglione et al., 2017), vendar pa nove tehnološke rešitve sprožajo vprašanja o zanesljivosti rezultatov digitalne forenzične preiskave, ki so aktualna tudi zaradi sistemsko neurejenih temeljev te forenzične discipline (odsotnost standardizacije postopkov, validacije in verifikacije digitalnih forenzičnih orodij in izobraževanja oziroma certificiranja preiskovalcev). Umanjkanje te ureditve je pereče, saj so napredne rešitve primarno tehnične narave, o čemer pravniki ne vedo veliko, niti ne razumejo delovanja digitalnih forenzičnih orodij, da bi lahko v kazenskem postopku samostojno in verodostojno odločali o zanesljivosti izsledkov digitalnih forenzičnih preiskav oziroma digitalnih dokazov.

V dobi velikega podatkovja se pospešenemu uvajanju avtomatizacije v digitalne forenzične preiskave ne glede na njene pomanjkljivosti ni (več) mogoče izogniti. Pri tolmačenju izsledkov tovrstne preiskave za potrebe kazenskega postopka pa je in bo potrebna določena mera previdnosti in upoštevanje specifik tako avtomatiziranih digitalnih forenzičnih orodij kot digitalnih dokazov. Rešitve je torej treba iskati v identifikaciji relevantnih vprašanj in pravilnem razumevanju narave digitalnega forenzičnega procesa, pri čemer mora biti učinkovitost oziroma hitrost digitalne forenzične preiskave ustrezno uravnotežena z njeno kakovostjo, postopek preiskave pa transparenten ne samo s procesnega, ampak tudi z vsebinskega vidika. Odločevalcu (predvsem sodniku) morajo biti v konkretnem primeru na voljo vse bistvene informacije o načinu oziroma postopku pridobitve določenega digitalnega dokaza, saj lahko le tako v okviru načela proste presoje dokazov verodostojno in pravilno presodi ta dokaz. Pri tem ostajajo ključni digitalni forenzični preiskovalci, ki morajo v celoti poznati in imeti nadzor nad delovanjem digitalnega forenzičnega orodja, ki ga uporabljajo pri preiskavi; niso pa s tega vidika zanemarljiva niti mnenja, da bi bilo treba v izobraževanje prihodnjih in mladih pravnikov vključiti osnove računalniškega programiranja, saj bodo le tako lahko razumeli podatkovno analitiko in umetno inteligenco, ki na različne načine čedalje bolj vplivata tudi na kazenske in druge pravne postopke (Contreras in McGarth, 2020), ter od digitalnih forenzikov znali zahtevati podatke, ki jih potrebujejo za odločanje.

Skratka – tako na pravnem kot na tehničnem področju se je treba zavedati, da avtomatizirana digitalna forenzična orodja niso popolna, zato mora biti njihova uporaba transparentna, dobro načrtovana in strokovna, ocena njihovih izsledkov pa temeljiti na dobrem poznavanju njihovih značilnosti in zmožnosti. Dokler digitalna forenzična znanost ne najde univerzalne metodologije, na podlagi katere bosta možni znanstvena validacija in verifikacija digitalnih forenzičnih orodij in tudi digitalnih dokazov, je bistveno, da digitalna forenzična preiskava v celoti ostane v domeni oziroma (skoraj dobesedno) v rokah digitalnih forenzičnih preiskovalcev. Dokler države ne vzpostavijo preverjenega modela za kvalificiranje oziroma certificiranje digitalnih forenzičnih preiskovalcev, pa morajo in bodo morali odločevalci v kazenskem postopku (predvsem sodniki) po potrebi prevzeti breme odločanja o kakovosti izvedene digitalne forenzične preiskave v konkretnem primeru, kar zahteva stalno nadgrajevanje njihovega znanja, saj lahko le tako v okviru načela iskanja resnice in načela proste presoje dokazov kritično, a prav(ično) ocenijo pravno dopustnost in dokazno (polno)vrednost ter v tem okviru zanesljivost digitalnih dokazov.

Literatura

1. Adedayo, O. M. (2016). Big Data and digital forensics. Rethinking Digital Forensics. *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*. Pridobljeno na https://ieeexplore.ieee.org/document/7740422
2. Al Fahdi, M., Clarke, N. L., Li, F. in Furnell, S. M. (2016). A suspect-oriented intelligent and automated computer forensic analysis. *Digital Investigation, 18*, 65–76.
3. Arshad, H., Bin Jantan, A. in Oludare, I. A. (2018). Digital forensics: Review of issues in scientific validation of digital evidence. *Journal of Information Processing Systems, 14*(2), 346–376.
4. Barmpatsalou, K., Cruz, T., Monteiro, E. in Simoes, P. (2018). Current and future trends in mobile device forensics: A survey. *ACM Computing Surveys, 51*(3), 1–31.

5. Bench-Capon, T. (2020). *The need for good old-fashioned AI and law.* Pridobljeno na https://cgi.csc.liv.ac.uk/~tbc/publications/erichRef.pdf
6. Bhat, W. A., AlZahrani, A. in Wani, M. A. (2021). Can computer forensic tools can be trusted in digital investigations? *Science & Justice, 61*(2), 198–203.
7. Borhaug, T. S. (2019). *The paradox of automation in digital forensics*. Trondheim: NTNU, Norwegian University of Science and Technology. Pridobljeno na https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2617753?show=full
8. Bryce, C. E., McDougle, R. D. in Roberstson, J. (2017). Digital forensics. V L. J. Moriarty (ur.), *Criminal justice technology in the 21st century* (3rd ed.) (str. 115–136). Springfield: Charles C. Thomas Pub Ltd.
9. Butterfield, E., Dixon, M., Miller, S. in Schreuder, Z. C. (2018). *Automated digital forensics.* Pridobljeno na http://eprints.leedsbeckett.ac.uk/id/eprint/5073/
10. Casey, E. (2019). Trust in digital evidence. *Digital Investigation 31.* Pridobljeno na https://doi.org/10.1016/j.fsidi.2019.200898
11. Caviglione, L., Wendzel, S. in Mazurczyk, W. (2017). The future of digital forensics: Challenges ad the road ahaed. *IEEE Security and Privacy Magazine, 15*(6), 12–17.
12. Contreras, A. in McGarth, J. (2020). Law, technology and pedagogy: Teaching coding to build a »future-proof« lawyer. *Minnesota Journal of Law, Science & Technology, 21*(2), 297–332.
13. Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579, US Supreme Court. (1993). Pridobljeno na https://supreme.justia.com/cases/federal/us/509/579/
14. DeMatteo, D., Fishel, S. in Tansey, A. (2019). Expert evidence: The (unfulfilled) promise of daubert. *Psychological Science in the Public Interest, 20*(3), 129–134.
15. Dežman, Z. (2013). Dokazna pravila in status resnice v kazenskem postopku. *Zbornik Preiskovanje in dokazne prepovedi – kazensko-pravni in kriminalistični vidiki* (str. 53–69). Ljubljana: Fakulteta za varnostne vede.
16. Dimpe, P. M. in Kogeda, O. P. (2019). A model for evaluating digital forensic tools. *Journal of Engineering and Applied Sciences, 14*(19), 7048–7058.
17. Direktiva 98/79/ES Evropskega parlamenta in Sveta z dne 27. oktobra 1998 o in vitro diagnostičnih medicinskih pripomočkih. (1998). *Uradni list Evropske unije*, (L/331).
18. Dixon, H. B. (2020). What judges and lawyers should understand about artificial intelligence technology? *Judges' Journal, 59*(1), 36–38.
19. Dogša, T. (1993). *Verifikacija in validacija programske opreme*. Maribor: Tehniška fakulteta, Elektroethnika, računalništvo in informatika.
20. European Network for Forensic Science Institutes (ENFSI). (2015). *Best practice manual for the forensic examination of digital technology.* Pridobljeno na https://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf
21. Evropska agencija za kibernetsko varnost. (2015). *Electronic evidence – A basic guide for first responders*. Pridobljeno na https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders
22. Flandrin, F., Buchanan, W. J., Macfarlane, R. J., Ramsay, B. in Smales, A. (2014). *Evaluating digital forensic tools (DFTs).* Pridobljeno na https://www.napier.ac.uk/~/media/worktribe/output-178532/flandrinpdf.pdf
23. Forensic Science Regulator. (2020). *Forensic Science Regulator guidance: Method validation in digital forensics, FSR-G-218.* Pridobljeno na https://assets.publishing.service.gov.uk/government/uploads/system/ uploads/attachment_data/file/921392/218_Method_Validation_in_Digital_Forensics_Issue_2_New_Base_Final.pdf
24. Garfinkel, S. (2010). Digital forensics research: The next 10 Years. *Digital Investigation 7*, S64–S73.
25. Geradts, Z. (2018). Digital, big data and computational forensics. *Forensic Sciences Research, 3*(3), 179–182.
26. Homem, I. (2018). *Advancing automation in digital forensic investigations.* Stockholm: Stockholm University.
27. Horsman, G. (2020). *ACPO principles for digital evidence: Time for an update?* Pridobljeno na https://doi.org/10.1016/j.fsir.2020.100076
28. Inštitut za slovenski jezik Frana Ramovša ZRC SAZU – Portal BOS. (2020). *Slovar slovenskega knjižnega jezika.* Pridobljeno na http://bos.zrc-sazu.si/sskj.html
29. Iqbal, S. in Alharbi, S. A. (2019). *Advancing automation in digital forensic investigations using machine learning forensics.* Pridobljeno na https://www.intechopen.com/books/digital-forensic-science/advancing-automation-in-digital-forensic-investigations-using-machine-learning-forensics
30. James, J. I. in Gladyshev, P. (2013). *Challenges with automation in digital forensics.* Pridobljeno na https://arxiv.org/abs/1303.4
31. Kishore, N., Saxena, S. in Raina, P. (2017). Big data as challenge and opportunity in digital forensic investigation. *2017 2nd International Conference on Telecommunication and Networks (TEL-NET).* Pridobljeno na https://ieeexplore.ieee.org/document/8343573
32. Larry, D. in Lars, D. (2011). *Digital forensics for legal professionals: Understanding digital evidence from the warrant to the courtroom*. Cambridge: Syngress.
33. Lillis, D., Becker, B. A., O'Sullivan, T. in Scanlon, M. (2016). *Current challenges and future research areas for digital forensic investigation.* Pridobljeno na https://arxiv.org/abs/1604.03850
34. Lopez, E. M., Moon, S. Y. in Park, J. H. (2016). Scenario-based digital forensics challenges in cloud computing. *Symmetry, 8*(10), 1–20.
35. Marturana, F., Tacconi, S., Berte, R. in Me, G. (2012). Triage-based automated analysis of evidence in court cases of copyright infringement. *2012 IEEE International Conference on Communications (ICC).* Pridobljeno na https://ieeexplore.ieee.org/document/6364819
36. Ministrstvo za notranje zadeve, Policija. (2021). *Poročilo o delu policije za leto 2020.* Ljubljana: Ministrstvo za notranje zadeve, Policija.
37. Mohammed, H., Clarke, N. in Li, F. (2016). An automated approach for digital forensic analysis of heterogeneous Big Data. *The Journal of Digital Forensics, Security and Law, 11*(2), 137–152.
38. Pravilnik o temeljnih kvalifikacijah za voznike motornih vozil v cestnem prometu. (2010). *Uradni list RS,* (103/10).
39. Qi, M., Liu, Y., Lu, L., Liu, J. in Li, M. (2014). Big Data management in digital forensics. *2014 IEEE 17th International Conference on Computational Science and Engineering*. Pridobljeno na https://ieeexplore.ieee.org/document/7023585
40. Selinšek, L. (2010). Digitalni dokazi v kazenskem postopku: pogledi na aktualna vprašanja. V A. Završnik (ur.), *Kriminaliteta in tehnologija: kako računalniki spreminjajo nadzor in zasebnost, ter kriminaliteto in kazenski pregon?* (str. 97–119). Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti.
41. Selinšek, L. (2011). Računalniška kriminaliteta in reševanje problemov iz prakse. *Pravosodni bilten, 32*(2), 223–237.
42. Selinšek, L. (2020). Osnove dokaznega prava s poudarkom na digitalnih dokazih. *Zbornik 1. Konference prava informacijske varnosti* (str. 34–48). Ljubljana: Lexpera, GV založba.

43. Shalaginov, J., Johnsen, J. W. in Franke, K. (2017). Cyber crime investigations in the era of Big Data. *2017 IEEE International Conference on Big Data*. Pridobljeno na https://ieeexplore.ieee.org/abstract/document/8258362
44. Shanmugam, K., Powell, R. in Owens, T. (2011). An approach for validation of digital anti-forensic evidence. *Information Security Journal: A Global Perspective, 20*(4-5), 219–230.
45. Šugman Stubbs, K., Gorkič, P. in Fišer, Z. (2020). *Temelji kazenskega procesnega prava*. Ljubljana: GV založba.
46. Svet Evrope. (1950). *Evropska konvencija o človekovih pravicah*. Pridobljeno na https://www.echr.coe.int/documents/convention_slv.pdf
47. Svet Evrope. (2020). *Electronic evidence guide – A basic guide for police officers, prosecutors and judges (Version 2.1.)*. Pridobljeno na https://rm.coe.int/c-proc-electronic-evidence-guide-2-1-en-june-2020-web2/16809ed4b4
48. Tehnopedia. (2020). *Automation.* Pridobljeno na https://www.techopedia.com/definition/32099/automation
49. Van Baar, R. B., van Beek, H. M. A. in van Eijk, E. J. (2014). Digital forensics as a service: A game changer. *Digital Investigation, 11*(1), S54–S62.
50. Van Beek, H. M. A., van Eijk, E. J., van Baar, R. B., Ugen, M., Bodde, J. N. C. in Siemelink A. J. (2015). Digital forensics as a service: Game on. *Digital Investigation, 15*(1), 20–38.
51. Varga, M. (2018). 9 mitov o strojnem učenju. *Revija Monitor, 05/2018*. Pridobljeno na https://www.monitor.si/clanek/9-mitov-o-strojnem-ucenju/185235/
52. Veber, J., in Smutny, Z. (2015). Standard ISO 27037:2012 and collection of digital evidence: Experience in the Czech Republic. *14th European Conference on Cyber Warfare & Security*. Pridobljeno na https://www.researchgate.net/publication/283226153_Standard_ISO_270372012_and_Collection_of_Digital_Evidence_Experience_in_the_Czech_Republic
53. Vincze, E. A. (2016). Challenges in digital forensics. *Police practice and Research, 17*(2), 183–194.
54. Vrhovno državno tožilstvo Republike Slovenije. (2021). *Skupno poročilo o delu državnih tožilstev 2020*. Ljubljana: Vrhovno državno tožilstvo Republike Slovenije.
55. Zakon o prevozih v cestnem prometu (ZPCP-2). (2006). *Uradni list RS*, (6/16).
56. Završnik, A. (2017). Algoritmično nadzorstvo: veliko podatkovje, algoritmi in družbeni nadzor. *Revija za kriminalistiko in kriminologijo 68*(2), 135–149.
57. Završnik, A. (2020). Criminal justice, artificial intelligence systems, and human rights. *ERA-Forum: scripta iuris europaei, 20*(4), 567–583.
58. Zawoad, S. in Hasan, R. (2015). Digital forensics in the age of Big Data: Challenges, approaches and opportunities. *2015 IEEE 17th International Conference on High Performance Computing and Communications.* Pridobljeno na https://ieeexplore.ieee.org/document/7336350

The Impact of Automation of Digital Forensic Investigations on Evidence in Criminal Proceedings

Lilijana Selinšek, Ph.D., Assistant Professor, Researcher, Institute of Criminology at the Faculty of Law Ljubljana, Slovenia.
E-mail: liljana.selinsek@pf.uni-lj.si

This article provides a brief insight into the challenges and dilemmas posed in the field of digital forensics by the steady increase of the number of electronic devices and their storage capacities, the ubiquitous use and connection of these devices, and the large amount of data they create. Digital forensic investigations today often involve a large number of devices and huge amounts of data. Due to limited personal and technical resources, many countries worldwide face investigative backlogs that negatively affect the principle of a trial occurring within a reasonable time. The investment of time and resources in a digital forensic investigation is often disproportionate to the results of this investigation, as more devices and data do not necessarily mean more digital evidence but only more material to be investigated. The needle, therefore, remains mainly the same, but the haystack in which it is sought is growing. One of the solutions being developed to address this problem is the (partial) automation of digital forensic investigations. This article presents a theoretical analysis of the current situation in this field, with special attention given to the question of how automation (i.e., machine or programmed investigation) impacts the reliability of such an investigation for the need of criminal proceedings. Until the concept of validation and formal verification of digital forensic tools is established globally, it is important for digital forensic researchers to have full control over all phases of the digital forensic investigation; and for decision-makers in criminal proceedings (especially public prosecutors and judges) to be aware of both the advantages and disadvantages of (partly) automated digital forensic tools.

Keywords: digital forensics, automation in digital forensics, digital evidence, digitalization of crime, socialization of technology, big data

UDC: 343.983.2:343.1