Domstolarnas utredningsansvar vid digital manipulation

Av tingsnotarien Elvira Landberg[1]

I en tid där digital manipulation, som deepfakes, snabbt utmanar tillförlitligheten hos bevis som presenteras i domstol ställs rättsväsendet inför nya prövningar. Hur påverkas domstolarnas utredningsansvar och principerna för bevisvärdering när gränsen mellan sanning och illusion suddas ut? Med utgångspunkt i svensk och internationell reglering och praxis analyseras de utmaningar som rättsväsendet kan komma att stå inför i en alltmer digital värld.

1 Inledning

Den tekniska utvecklingen har alltid utmanat rättssystemet men få innovationer har haft samma potentiella inverkan som den senaste generationen av manipulationsverktyg. Det går med dagens teknik att skapa en så kallad *deepfake*. En deepfake är en film, video, eller bild som har skapats med hjälp av teknik, såsom AI, och som kan se mycket autentisk ut.[2] Möjligheten att med hög precision manipulera bilder, videor och ljud innebär en ny form av osäkerhet kring autenticiteten hos digitala bevis. Det här ställer därför nya krav på domstolarnas förmåga att identifiera manipulerade bevis och säkerställa rättssäkerhet vid bevisvärderingen.

Sedan införandet av reformen *En modernare rättegång* på 2000-talet övergick domstolarna till att bland annat introducera videoteknik i domstolsförhandlingar och spela in förhör digitalt.[3] Från att tidigare ha förlitat sig på kassettbandspelare möjliggjorde de digitala framstegen uppspelning av underinstansens förhör i överinstansen. Reformen krävde omfattande tekniska installationer men idag används tekniken inte bara för inspelningar utan också för att låta parter delta på distans, vilket ytterligare har effektiviserat rättsprocessen. Under de senaste 20 åren har det skett en enorm teknisk utveckling i samhället som fortsatt påverkar rättsväsendet.

Deepfake-teknologi har snabbt utvecklats från en teknisk kuriositet till ett potentiellt hot mot rättvisa bedömningar vid bevisvärderingar. Deepfakes används redan i försök att förvränga verkligheten för att exempelvis påverka människors politiska uppfattning. I mars 2022 lades en deepfake i form av ett videoklipp upp på internet där Ukrainas

[1] Författaren tjänstgör vid Ångermanlands tingsrätt.
[2] Se Internetkunskaps ordlista, https://internetkunskap.se/artiklar/ordlista/deepfake/.
[3] *En modernare rättegång — reformering av processen i allmän domstol*, prop. 2004/05:131; Se Thorblad, B., Holmgren, M., Domstolsverket — från starten till våra dagar i *SvJT* 2018 s. 16–35, https://svjt.se/svjt/2018/16.

president Volodymyr Zelenskyj uppmanade sina landsmän att lägga ner sina vapen.[4] Det går inte längre att lita på att den röst som hörs eller den bild som visas digitalt är det som den utger sig för att vara. Tekniken kan i dagsläget redan skapa falska digitala vittnesmål och kompromettera individer genom fabricerade videor. Vid bedrägeriförsök används deepfakes för att i telefonsamtal lura personer att de talar med någon de känner.[5] Den här utveckling innebär också att digitala bevis, som tidigare har kunnat betraktats som relativt objektiva, riskerar att förlora sin ställning som tillförlitliga.

Frågan om hur rättens utredningsansvar påverkas av denna teknologiska utveckling är högaktuell. Hur långtgående är ansvaret när rätten ställs inför bevis som kan ha manipulerats på ett sätt som är svårt att upptäcka? Vilka rättsliga och tekniska åtgärder kan säkerställa att manipulation upptäcks? Syftet med den här artikeln är att analysera dessa frågor och diskutera möjliga vägar framåt för att stärka rättssäkerheten i ljuset av de teknologiska utmaningarna kopplat till bevisvärdering.

2 Utmaningar med deepfake

I och med den tekniska utvecklingen i samhället har digitala bevis på senare år fått en alltmer central roll. E-postmeddelanden, bilder, videor och ljudinspelningar används ofta för att styrka eller motbevisa olika påståenden. Skriftliga bevis har ofta betraktats som särskilt tillförlitliga då de saknar den subjektivitet som muntliga vittnesmål kan präglas av.[6] Teknisk bevisning har även tidsstämplar och annan bakgrundsdata som ytterligare förstärker bevisets robusthet. Utvecklingen av manipulationstekniker som deepfakes rubbar dock detta. Till skillnad från tidigare former av manipulering som exempelvis klippning av videor eller ändring av textdokument kan deepfakes skapa en så verklighetstrogen representation av en händelse att den är mycket svår att skilja från autentiska bevis — även för experter.[7]

Rättens uppgift att värdera bevis påverkas av deepfakes på två avgörande sätt. Dels går det att ifrågasätta robustheten av ett bevis, dels krävs en ökad kunskap kring tekniskt komplexa system.[8] När digital manipulation inte längre är tidskrävande eller särskilt svårt att genomföra tvingas rätten att förhålla sig skeptiska till de bevis som inte kan presenteras med en utförlig bakgrundsdata. För att avgöra huruvida ett bevis är äkta kan domstolen behöva ta hjälp av teknisk expertis eller ha

[4] Se videon på Forskning.se, https://www.forskning.se/2022/06/02/darfor-troddeingen-pa-videon-dar-zelenskyj-gav-upp/.
[5] Westfall, C., AI Deepfakes On The Rise Causing Billions In Fraud Losses i *Forbes*, https://www.forbes.com/sites/chriswestfall/2024/11/29/ai-deepfakes-of-elon-musk-on-the-rise-causing-billions-in-fraud-losses/, 2024.
[6] Se Ekelöf, P. O., Edelstam, H., Heuman, L., *Rättegång IV*, 7 uppl., Stockholm: Nordstedts Juridik, 2009, s. 255.
[7] Se Stockholms universitets nyhet *Hur rädda ska vi vara för deep fakes?*, https://www.su.se/nyheter/hur-r%C3%A4dda-ska-vi-vara-f%C3%B6r-deep-fakes-1.651115.
[8] För fördjupning om robusthet se Ekelöf, P. O., Edelstam, H., Heuman, L., *Rättegång IV*, 7 uppl., Stockholm: Nordstedts Juridik, 2009, s. 187–189.

tillgång till avancerade verktyg, vilket i praktiken även kan leda till förlust av effektivitet i processer.

Det finns dessutom en annan problematik med deepfakes som läggs fram som bevis i en domstolsprocess. Juridiska experter framhåller fenomenet ”lögnarens vinst”[9], där en misstänkt kan hävda att bevismaterial, till exempel en video- eller ljudinspelning, är manipulerat eller falskt även när det inte är det.[10] Det kan påverka effektiviteten vid lagföring av brott, eftersom åklagaren behöver bevisa att bevisningen är äkta och inte har blivit manipulerad.

3 Bevisvärdering i ljuset av digital manipulation

3.1 Fri bevisprövning

Bevisvärderingen i svensk rätt bygger på principen om fri bevisprövning vilken stadgas i 35 kap. 1 § rättegångsbalken. Det finns ingen lagstiftning som uttryckligen beskriver hur prövningen ska gå till eller hur olika bevis ska tillmätas betydelse, utan det regleras till största del genom praxis. Rätten är fri att bedöma bevisens robusthet och styrka utifrån omständigheterna i det enskilda fallet. I dispositiva mål bär parterna i regel ansvaret för att presentera och styrka sin talan medan åklagaren och rätten i indispositiva mål bär ett ansvar för att utredningen är tillräcklig. Utredningsansvaret innebär att rätten ska se till att ett mål är tillräckligt utrett för att kunna avgöras. Vid en misstänkt digital manipulation av bevis kan utredningsansvaret exempelvis innebära att rätten aktivt måste ifrågasätta och undersöka bevisens äkthet. Frågan blir då hur bevisprövningen ska ske när det blir allt svårare att avgöra om bevis är äkta. Flexibiliteten vid bevisvärderingen möjliggör en helhetsbedömning där hänsyn kan tas till alla relevanta faktorer. Samtidigt innebär den fria bevisprövningen att rätten och de övriga aktörerna i domstol bär ett stort ansvar för att upptäcka och hantera brister i bevismaterialet.

I svensk rätt finns ingen lagstadgad reglering av hur rätten ska hantera frågor om bevismanipulation. I Högsta domstolens praxis framkommer generellt att bevis som är framlagda i straffprocesser ska bedömas utifrån deras trovärdighet, relevans och styrka i förhållande till andra bevis i målet och att det ska vara ”ställt bortom rimligt tvivel” att någon är skyldig till brott för att dömas.[11] Bevisens autenticitet måste bedömas utifrån omständigheterna i det enskilda fallet, inklusive tekniska möjligheter till manipulation.

[9] *Eng*: liar’s dividend; Se Lindblad, T., *Därför trodde ingen på videon där Zelenskyj gav upp* på Forskning.se, https://www.forskning.se/2022/06/02/darfor-trodde-ingen-pa-videon-dar-zelenskyj-gav-upp/.

[10] Se European Parliamentary Research Services studie *Tackling deepfakes in European policy,* https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf?fbclid=IwZXh0bgNhZW0CMTEAAR1Z6D8H1ZXpXm7ZAk0VSEqtwoVyBuYWYetXUP6sswh1LWMd8PhXxSJ39os_aem_5ZU31YuJvaQPOnTzSrIvqg#page73, 2021 s. 55; Se även Venema, A., Geradts, Z., Digital Forensics, Deepfakes, and the Legal Process i The SciTech Lawyer, 2020.

[11] Se exempelvis NJA 1980 s. 725.

I NJA 2023 s. 29 (I och II) underströk Högsta domstolen vikten av att en bevisprövning ska inkludera en grundlig analys av individuella bevis i en beviskedja och en värdering av deras sammantagna betydelse. Även om dessa fall inte explicit rörde digitalt manipulerad bevisning klargjordes att alla rimliga alternativa förklaringar måste uteslutas för en fällande dom. Det här kan bli relevant för kommande bedömningar av deepfake-material, där trovärdigheten av digitala bevis måste granskas noggrant både individuellt och som en del av en helhet. Högsta domstolen förtydligar även att beviskravet i brottmål innebär att utredningen måste vara så pass heltäckande att det inte finns skäl att tro att ytterligare utredning skulle kunna leda till en annan slutsats. Högsta domstolen betonar vikten av att utredningen är robust och tillförlitlig, vilket kan bli svårare att uppnå vid en användning av misstänkt digitalt manipulerade bevis.

Det finns även tvistemålspraxis från hovrätten och Högsta domstolen där rätten behandlar frågor om beviskrav och bevisbördans placering rörande invändningar om förfalskade underskrifter. Detta kan relateras till frågan om hur beviskravet för misstänkt manipulerad bevisning ska hanteras. Senare avgöranden från Högsta domstolen kan tala för att bevisbördan numera generellt bör placeras på den som påstår att en förfalskning av underskrifter har skett.[12] I RH 2014:27 framhåller dock hovrätten att de aktuella avgörandena från Högsta domstolen inte bör tillmätas en generell räckvidd utan att utgångspunkten fortsatt, i enlighet med ett rättsfall från 1976, är att borgenären, med ett lägre beviskrav, har bevisbördan vid invändning om förfalskning.[13] Enligt hovrätten har Högsta domstolen i de senare fallen beaktat särskilda omständigheter när bevisbördan lagts på gäldenären och inte givit några uttalanden som ger stöd för att det skulle vara en ny generell regel. Rättsläget är således oklart, men enligt doktrin ska den som påstår att en namnteckning är äkta i regel ha bevisbördan.[14] Dock med ett lägre beviskrav.

Ett aktuellt fall från Förvaltningsrätten i Göteborg visar även på de svårigheter som kan uppstå med att hantera digitala beslutssystem och bristande insyn i algoritmiskt genererade beslut.[15] Den här problematiken kring insyn och teknisk kunskap i rätten speglar utmaningar som är kopplade till manipulation av digitala bevis eftersom den belyser att det krävs verktyg och kompetens för att granska digitalt material på ett rättssäkert sätt.

[12] Se NJA 2008 s. 890 och NJA 2009 s. 244; Se bland annat Svea hovrätts domar den 16 november 2011 i mål nr T 6836-10 och den 2 januari 2012 i mål nr T 6564-11; Se Ekelöf, P. O., Edelstam, H., Heuman, L., *Rättegång IV*, 7 uppl., Stockholm: Nordstedts Juridik, 2009, s. 131–133.
[13] Se NJA 1976 s. 667.
[14] Jfr RH 2013:16.
[15] Se Förvaltningsrätten i Göteborgs dom den 27 augusti 2020 i mål nr FR 6541-20; Se Kronblad, C., Algoritmisk orättvisa — Göteborgs felkodade algoritm för skolplaceringar i Fjaestad, M., Vinge, S., *AI & makten över besluten*, Stockholm: Volante, 2024 s. 25–46.

3.2 Notoriska fakta i den digitala tidsåldern

Notoriska fakta, eller fakta som är allmänt känd och inte kräver bevisning, har en grundläggande roll i svensk processrätt.[16] Omedelbarhetsprincipen är lagstadgad och enligt 35 kap. 2 § rättegångsbalken får rätten inte grunda sina avgöranden på annat än det som framkommit i processen med undantag för fakta som är notoriska. Principen innebär att domstolar kan ta hänsyn till allmänt kända omständigheter utan att dessa behöver åberopas av parterna eller styrkas genom bevis.

I den digitala tidsåldern utmanas dock gränsen för vad som kan anses vara notoriska fakta. Förekomsten av desinformation, deepfakes och manipulationstekniker innebär att fakta som tidigare kunde betraktas som självklar eller allmänt känd nu kan vara föremål för manipulation. Exempelvis kan en viral video som framstår som autentisk utgöra en del av den allmänna kunskapen, men dess äkthet kan ifrågasättas i en rättslig kontext.

Den ökande tillgången till verktyg för att manipulera digitalt material innebär också att rättsliga aktörer måste vara pålästa om vad som i rättssalen ska anses vara notoriska fakta. En bild eller video som spridits i sociala medier eller som visar en konversation mellan två personer kan vara en fabricerad representation. Det ställer krav på att rätten kritiskt granskar sådant material även om det vid första anblick framstår som otvetydigt vad som visas upp. Rätten behöver också följa med i den tekniska utvecklingen för att ha tillräckligt med notorisk kunskap i dagens digitala värld. I en digital kontext kan notoriska fakta behöva omdefinieras.

4 Europeisk reglering av digital manipulation

EU har de senaste åren intensifierat sitt arbete med att reglera digital manipulation, med fokus på både integritet, säkerhet och demokratisk stabilitet. För att reglera digital manipulation har EU skapat flera rättsakter bland annat AI-förordningen,[17] förordningen om digitala tjänster[18] (DSA) och förordningen om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden[19] (eIDAS). Även Europakonventionen om skydd för de mänskliga rättigheterna (EKMR) är relevant vid en bevisvärdering där det

[16] Se Ekelöf, P. O., Edelstam, H., Heuman, L., *Rättegång IV*, 7 uppl., Stockholm: Nordstedts Juridik, 2009, s. 59.

[17] Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens).

[18] Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG (förordningen om digitala tjänster).

[19] Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG.

finns misstanke om manipulerad bevisning, eftersom artikel 6 EKMR stadgar rätten till en rättvis rättegång.

4.1 AI-förordningen — Ett ramverk för ansvarsfull AI

AI-förordningen, som trädde i kraft 1 augusti 2024, syftar till att reglera utveckling och användning av AI-baserade teknologier.[20] Förordningen delar in AI-system i olika risknivåer och placerar deepfakes i kategorin som kräver transparens.[21] I artikel 50 p. 4 AI-förordningen stadgas att deepfake-innehåll tydligt måste märkas som artificiellt genererat för att minimera risken för vilseledning.

I en juridisk kontext kan detta regelverk få betydelse i svenska rättsprocesser där deepfake-bevis förekommer. Om ett deepfake-material inte uppfyller AI-förordningens krav på transparens kan det påverka det digitala bevisets robusthet vid rättens bevisvärdering. Dessutom kan aktörernas skyldigheter att implementera mekanismer för att verifiera autenticiteten av AI-genererat innehåll bli en faktor vid prövningen av bevisens digitala ursprung.

4.2 DSA — Reglering av plattformar och spridning av manipulation

DSA, som sedan februari 2024 gäller för alla plattformar, stärker ansvaret för onlineplattformar att motverka spridning av olagligt eller skadligt innehåll.[22] Dessa plattformar kan exempelvis vara sociala medier. Syftet med DSA är att ”*bygga en säkrare och rättvisare online-värld*”.[23] Enligt artikel 9 DSA måste plattformar identifiera och begränsa spridningen av olagligt innehåll som potentiellt kan skada samhällsintressen eller individers rättigheter.

DSA får betydelse i en svensk bevisvärderingskontext då manipulativa bevis som kan användas i en rättsprocess ofta sprids eller hittas på digitala plattformar. Om en plattform inte vidtagit tillräckliga åtgärder för att identifiera och märka deepfakes kan det påverka bevisens robusthet. DSA kan också ge rättstillämpare ett verktyg för att kräva information från plattformar om materialets ursprung och metadata.

4.3 eIDAS

EU:s eIDAS-förordning utgör en viktig rättslig ram för elektronisk identifiering och tillförlitliga tjänster för elektroniska transaktioner inom unionen. Syftet med förordningen är att skapa en harmoniserad standard för att bygga förtroende för digitala lösningar, särskilt när det gäller elektroniska underskrifter, tidsstämpling, elektroniska sigill och

[20] Bestämmelserna börjar dock tillämpas vid olika tidpunkter.
[21] Se Europaparlamentets artikel *EU:s AI-lag: första lagstiftningen om artificiell intelligens,* https://www.europarl.europa.eu/topics/sv/article/20230601STO93804/eu-s-ai-lag-forsta-lagstiftningen-om-artificiell-intelligens.
[22] Se Europeiska kommissionens information om förordningen, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_sv.
[23] Se Europeiska kommissionens frågor och svar om förordningen, https://digital-strategy.ec.europa.eu/sv/faqs/digital-services-act-questions-and-answers.

andra tjänster som kan vara centrala vid autentisering och verifiering av digitalt material. Förordningen spelar därmed en viktig roll när det gäller att säkerställa tillförlitligheten hos digitala bevis i rättsliga sammanhang.

Ett av de mest relevanta områdena i förhållande till bevisvärdering är regleringen av avancerade och kvalificerade elektroniska underskrifter. Enligt artikel 25 eIDAS ska en kvalificerad elektronisk underskrift, som är verifierad enligt eIDAS-standarder, ha samma rättsliga status som en handskriven underskrift i samtliga medlemsstater. Den här typen av underskrifter kan exempelvis användas för att styrka autenticiteten och integriteten hos ett elektroniskt dokument vilket gör den särskilt betydelsefull vid rättstvister där äktheten av digitala handlingar ifrågasätts.

Förutom elektroniska underskrifter reglerar eIDAS även kvalificerade tidsstämplingar som kan vara relevanta vid bedömningen av när ett digitalt dokument har skapats eller ändrats.[24] Tidsstämplar kan bidra till att fastställa en digital beviskedja. En tidsstämpel kan verifiera att en video eller ett dokument inte har ändrats sedan en viss tidpunkt vilket stärker dess trovärdighet i domstol.

Det är dock viktigt att notera att eIDAS inte uttryckligen reglerar hur digitala bevis ska värderas i rättsprocesser. Det överlåts till medlemsstaternas nationella processrätt att bestämma regler för bevisvärdering och vilka krav som ska ställas på digitala bevis. Det är dock viktigt att säkerställa att rätten och övriga aktörer har den tekniska kompetens som krävs för att förstå och använda eIDAS-standarderna vid prövning av digitala bevis.

4.4 EKMR

Artikel 6 EKMR stadgar rätten till en rättvis rättegång och har därigenom en central roll i frågor som rör bevisning och rättssäkerhet. Enligt artikel 6 EKMR ska varje part ges en rimlig möjlighet att ifrågasätta bevis som läggs fram emot parten. Det gäller även om parten anser att beviset är falskt eller otillförlitligt. Om en inspelning, bild eller video används som bevismaterial ska den misstänkte ha rätt att granska och ifrågasätta bevisets äkthet. Det här innebär att rätten inte kan godta tekniskt framställda bevis utan att säkerställa dess äkthet genom en transparent och granskningsbar process. Artikel 6 EKMR föreskriver dock inte några detaljerade regler om bevisningens tillåtlighet eller bevisvärde; också dessa frågor överlåts till medlemsstaterna.

I ljuset av den tekniska utvecklingen kan kravet på en rättvis rättegång enligt artikel 6 EKMR innebära att nationella domstolar tvingas stärka sina processer kring granskningen av digital bevisning. Det kan exempelvis ske genom att i högre grad möjliggöra för parterna att anlita tekniska experter eller genom att rätten själv tillämpar tekniska verktyg och tillfrågar experter för att verifiera materialets autenticitet.

[24] Se artikel 41 eIDAS.

4.5 Praxis från Europa

I fallet Batiashvili mot Georgien[25] prövade Europadomstolen frågor rörande rätten till en rättvis rättegång enligt artikel 6 i EKMR. Irakli Batiashvili, en georgisk politiker, arresterades i juli 2006 och anklagades för att ha stöttat en väpnad grupp. Under utredningen avlyssnade myndigheterna telefonsamtal mellan Batiashvili och en medlem från den väpnade gruppen. Ett av dessa samtal sändes sedan i nationell TV, men Batiashvili hävdade att inspelningen hade manipulerats för att framställa honom på ett negativt sätt.

Domstolen fann att de georgiska myndigheterna hade påverkat allmänhetens uppfattning om Batiashvilis skuld genom att manipulera och sprida den avlyssnade konversationen innan en rättslig prövning hade ägt rum. Det här utgjorde därför ett brott mot vad som stadgas i artikel 6.2 EKMR.

Även om fallet inte explicit handlar om manipulerad bevisning där deepfake-teknologi använts så exemplifierar och belyser det de risker som finns vid bevisvärdering av digitala bevis, såsom ljudinspelningar. Användandet av manipulerande teknologi kan leda till kränkningar av de mänskliga rättigheterna, särskilt om det inte upptäcks, och det behövs därför en medvetenhet om vilken teknologi som kan användas för att manipulera bevisning.

5 Jämförelse med amerikansk rätt

5.1 Amerikansk lagstiftning

I det amerikanska rättssystemet regleras autentisering och identifiering av bevisning av regel 901 i *Federal Rules of Evidence*.[26] Denna regel fastställer att för att ett bevis ska anses tillåtet i domstol måste den part som åberopar beviset tillhandahålla tillräcklig grund för att visa att det är vad parten påstår att det är. Regeln är uppdelad i en allmän bestämmelse (a) och i en lista (b) över exempel på hur bevis kan autentiseras.

Enligt regel 901(a) krävs det att den som lägger fram ett bevis producerar tillräcklig bevisning för att stödja en slutsats om att föremålet är vad parten påstår att det är. I 901(b) listas flera exempel på hur bevis kan autentiseras. Det kan vara genom exempelvis vittnesmål från en person med kunskap, telefonkonversationer, äldre dokument m.m.[27]

I regel 702 samma lag regleras när och hur ett expertvittne kan vittna i en rättegång.[28] Enligt regeln får ett expertvittne ge sitt utlåtande om: specialiserad kunskap, tillförlitlighet, tillämplighet och korrekt tillämp-

[25] *Batiashvili v. Georgia*, nr. 8284/07, dom meddelad den 10 oktober 2019.
[26] Se fullständig lagtext på Legal Information Institutes hemsida, https://www.law.cornell.edu/rules/fre/rule_901.
[27] Se fullständig lagtext på Legal Information Institutes hemsida, https://www.law.cornell.edu/rules/fre/rule_901.
[28] Se fullständig lagtext på Legal Information Institutes hemsida, https://www.law.cornell.edu/rules/fre/rule_702.

ning.[29] Regeln finns för att säkerställa att expertvittnesmål är både trovärdiga och relevanta för att garantera en rättvis rättegång.

5.2 Amerikansk praxis

I USA finns det även praxis om så kallade Daubert-regler[30] som används för att bedöma om vetenskapliga expertutlåtanden uppfyller kriterierna för tillförlitlighet[31]. Dessa regler kan exempelvis tillämpas på expertutlåtanden om autenticiteten av digitala bevis. En sådan praxis kan jämföras med de sakkunnigutlåtanden som används i Sverige. Reglerna har sitt ursprung i fallet Daubert v. Merrell Dow Pharmaceuticals, Inc. som avgjordes av den amerikanska Högsta domstolen 1993.[32] Målet rörde frågan om vetenskapliga expertrapporter kunde användas som bevis.

Enligt vad som stadgas i Daubert-fallet är det domarens uppgift att avgöra om bevisningen är tillräckligt tillförlitlig för att presenteras inför en jury. I rättsfallet ställs det upp fyra kriterier för tillförlitlighet som domaren ska överväga när bevisningens vetenskapliga grund bedöms: om teorin eller metoden har testats, om den har varit föremål för peer review och publicering, om det finns en känd eller potentiell felmarginal och om standarder för metoden är etablerade samt om teorin eller metoden är allmänt accepterad inom det vetenskapliga samfundet.[33] Det betonades dock att listan över kriterierna inte är uttömmande och att rätten ska anpassa sin bedömning till det specifika fallet och den aktuella typen av bevis.

Efter Daubert-fallet har domstolar i USA använt dessa principer för att hantera vetenskapliga och tekniska bevis. Ett exempel är användningen av DNA-bevisning och digitala metoder som fingeravtrycksanalys, där metoderna utvärderas enligt dessa standarder. Det har efter Daubert-fallet kommit ytterligare två relevanta fall som har utvecklat reglerna. I General Electric Co. v. Joiner[34] klargjordes att domare har rätt att utesluta expertbevisning om de anser att den inte håller vetenskaplig standard och i Kumho Tire Co. v. Carmichael[35] utvidgades Daubert-reglerna till att omfatta teknisk bevisning och expertbevisning som inte bara är strikt vetenskaplig.

Genom att sätta internationell praxis och reglering i en svensk kontext kan det konstateras att reglering av bevisvärdering skiljer sig åt. När rätten i svenska domstolar ska bedöma misstänkt manipulerad

[29] Se fullständig lagtext på Legal Information Institutes hemsida, https://www.law.cornell.edu/rules/fre/rule_702.
[30] *Eng*: Daubert Standard.
[31] *Eng:* reliability.
[32] Målet finns tillgängligt att läsa i sin helhet via följande länk, https://supreme.justia.com/cases/federal/us/509/579/.
[33] Se Legal Information Institutes hemsida, https://www.law.cornell.edu/wex/daubert_standard.
[34] Målet finns tillgängligt att läsa i sin helhet via följande länk, https://supreme.justia.com/cases/federal/us/522/136/.
[35] Målet finns tillgängligt att läsa i sin helhet via följande länk, https://supreme.justia.com/cases/federal/us/526/137/.

bevisning behövs mer ledning än vad som finns i dagsläget. En sådan ledning behöver dock inte bestå av ny lag utan kan istället utkristalliseras och förtydligas genom vägledande praxis från Högsta domstolen såsom Högsta domstolen i USA har gjort med Daubert-reglerna.

6 Avslutande analys

Den teknologiska utvecklingen medför stora möjligheter men också omfattande utmaningar för rättsväsendet. Utvecklingen av avancerad manipulationsteknik, som deepfakes, sätter fokus på en central del av bevisvärderingen, vilken är att säkerställa trovärdigheten hos bevis som läggs fram i en rättsprocess. Svensk rätt utgår ifrån principen om fri bevisvärdering. Principen bygger dock på ett fundamentalt antagande — att bevisen som ligger till grund för prövningen faktiskt är äkta. Det tekniska landskapet som finns redan idag kräver anpassning och förnyelse. Förmågan att upptäcka och förstå manipulation av digitala bevis har blivit central, inte bara i brottmål utan också i civilrättsliga tvister där elektronisk kommunikation och digital dokumentation ofta är avgörande bevisning. Deepfakes ställer särskilt höga krav på både teknisk och juridisk kompetens.

6.1 En proaktiv strategi

På kort sikt krävs en proaktiv strategi för att stärka rättsväsendets förmåga att hantera digital bevisning. Forskning och utbildningsinsatser för domare och övriga rättsliga aktörer är avgörande för att säkerställa att det finns tillräcklig kunskap för att förstå hur digital manipulation fungerar och när det finns anledning att ifrågasätta bevisens autenticitet. Utbildningen bör exempelvis omfatta grundläggande teknisk kunskap om deepfake-teknologi, hur metadata analyseras samt vilka redskap som finns för att upptäcka manipulation.

Vidare måste domstolar ges tillgång till expertis och verktyg för att bedöma digitala bevis. Det kan exempelvis ske genom att bygga ut samarbeten med tekniska experter eller genom att etablera permanenta resurser inom rättsväsendet som är specialiserade på digital verifiering. Här kan också internationellt samarbete spela en viktig roll eftersom tekniska standarder och verifieringsverktyg ofta utvecklas i globala sammanhang.

6.2 Praxisutveckling

Det är sannolikt att praxis snart kommer att utvecklas inom det här området, särskilt när högre instanser får möjlighet att pröva mål där frågor om, och bedömning av, misstänkt manipulerade bevis är centrala. Högsta domstolen kan genom prejudikat fastställa vägledande principer för hur misstänkt manipulerade bevis ska hanteras, i likhet med den praxis som finns i exempelvis USA. Det kan även inkludera riktlinjer för när teknisk expertis bör anlitas och hur bevisbördan för äkthet ska fördelas mellan parterna.

Att domstolar tar en aktiv roll som ”gatekeepers” är också avgörande för att hantera frågan om notoriska fakta. I en digital tidsålder behöver det klargöras vad som är notoriska fakta och hur rätten bör hantera fakta som framstår som allmänt kända men som är resultatet av desinformation eller manipulation.

6.3 Balansgången mellan effektivitet och rättssäkerhet

Ett centralt dilemma är att hanteringen av digital manipulation inte får leda till att rättsprocessen blir onödigt komplicerad eller ineffektiv. För mycket fokus på teknisk granskning kan innebära högre kostnader och längre handläggningstider vilket i sig kan hota grundläggande rättsliga principer. Å andra sidan får domstolar inte förbise risken att manipulerade bevis påverkar målets utfall.

För att upprätthålla balansen krävs en mångfacetterad strategi där domstolar kombinerar teknisk expertis med en medvetenhet om bevisens begränsningar. En möjlig väg framåt är att införa tydligare reglering om när teknisk granskning är obligatorisk samt att utarbeta riktlinjer för vilka bevis som bör åtföljas av utförlig dokumentation om tekniskt ursprung.

Deepfake-teknologins utmaningar belyser behovet av att stärka rättsväsendets motståndskraft mot digital manipulation. Genom att prioritera utbildning, utveckling av vägledande praxis och investering i tekniska lösningar kan aktörerna i det svenska rättssystemet säkerställa att bevisvärderingen förblir rättssäker och effektiv. Den här anpassningen är inte bara en reaktion på teknologins framsteg, utan också en möjlighet att förnya och förstärka tilliten till rättsväsendet i en alltmer digitaliserad värld. Genom att agera proaktivt och utveckla verktyg för att hantera digital manipulation kan rättsväsendet fortsätta att vara en garant för rättssäkerhet även i en tid då gränsen mellan verklighet och fiktion ständigt prövas.