Ajalooline Ajakiri, 2025, 2 (192), 123–152

Digitaalse kultuuripärandi autentsuse tagamine

Kurmo Konsa

Digitaalse kultuuripärandi säilitamine on muutunud üheks keskseks raskuseks arhiivinduses ja laiemalt kogu MAR-sektoris (muuseumid, arhiivid ja raamatukogud)[1]. Üha enam kultuuriloolise väärtusega teavet tekib, levib ja talletub üksnes digitaalsel kujul, mistõttu on nende objektide autentsuse tagamine ja mõtestamine muutunud oluliseks küsimuseks nii teadlaste, kuraatorite kui ka poliitikakujundajate jaoks. Traditsioonilises arhiivinduses on autentsus seotud diplomaatikast pärit provenientsi (päritolu) ja tõendusväärtuse kontseptsioonidega. Nimetatud käsitluse kohaselt on dokument autentne, kui selle päritolu on tuvastatav ning sisu ja struktuur muutumatud.[2]

Digiobjektide puhul on klassikalised autentsuse käsitlused kahtluse alla seatud, kuna digiobjekt ei ole oma füüsilise kandjaga lahutamatult seotud. Seega digiobjektide puhul ei säilitata materiaalset ega ka mittemateriaalset objekti, millel on väärtused, vaid sotsiaalseid võrgustikke, mis ühendavad tähenduste ja väärtustega objekte inimeste ja ühiskondadega. Seetõttu on digiarhiivinduses autentsus nihkunud objektiomastelt tunnustelt institutsionaalsete ja protseduuriliste mehhanismide valdkonda. Samas puudub

[1] MAR-sektori kohta vt Kurmo Konsa, "Kas digitaalne infosüsteem ühtlustab teabeasutusi: muuseumide, arhiivide ja raamatukogude konvergents", *Ajalooline Ajakiri*, 1 (2023), 47–75.

[2] Vt nt Samuel Muller, Johan A. Feith, Robert Fruin, "Arhiivide korraldamise ja kirjeldamise käsiraamat", *Tuna*, 1 (1998), 91–105; 1 (1999), 109–121; 2 (1999), 73–87; 3 (1999), 117–124; 4 (1999), 115–120; 1 (2000), 125–132; 3 (2000), 113–121; 4 (2000), 98–107; 1 (2001), 49–53; 2 (2001), 132–139; 3 (2001), 107–114; Hilary Jenkinson, *A Manual of Archive Administration* (Oxford: Clarendon Press, 1922); *Arhiivinduse käsiraamat*, toim Otto Liiv (Tartu: Akadeemiline Kooperatiiv, 1933); Theodore R. Schellenberg, *Modern Archives Principles and Techniques* (Chicago: The University of Chicago Press, 1956); Luciana Duranti, "Diplomatics: New Uses for an Old Science, Part I", *Archivaria*, 28 (1989), 7–27; Luciana Duranti, "Reliability and Authenticity: The Concepts and Their Implications", *Archivaria*, 39 (1995), 5–10; Bernard Barbiche, "Diplomatics of Modern Official Documents (Sixteenth – Eighteenth Centuries): Evaluation and Perspectives", *The American Archivist*, 59:4 (1996), 422–436; Bruno Delmas, "Manifesto for a Contemporary Diplomatics: From Institutional Documents to Organic Information", *The American Archivist*, 59:4 (1999), 438–452; Raimo Pohjola, "Max Lehmann ja provenientsipõhimõtte areng", *Tuna*, 3 (2016), 61–78.

https://doi.org/10.12697/AA.2025.2.02

digiarhiivinduses endiselt üksmeel, milliseid omadusi pidada autentsuse seisukohalt määravaks ning kuidas neid usaldusväärselt säilitada.

Autentsus ei ole pelgalt tehniline ega arhiivinduslik kriteerium, vaid ajalooline, institutsionaalne ja kultuuriline konstruktsioon, mille säilitamine digitaalses keskkonnas eeldab teadlikke valikuid ja põhjendatud kompromisse. Kuidas seda aga teha? Kuidas siduda säilitamisprotsesse enam ühiskonnaga? Tegemist on keerukate küsimustega, millele sobivaimat vastust alles otsitakse. Olukord on eriti komplitseeritud kultuuripärandi valdkonnas, kus digiobjektid hõlmavad muuseumide dokumentatsioone, kuraatorinarratiive, virtuaalnäitusi, heli- ja visuaalfaile. Selliste objektide autentsust tuleb säilitada nii, et jääks alles ka nende kultuuriline ja semiootiline tähendusväli.

Käesoleva artikli eesmärk on näidata, kuidas on autentsuse mõiste kujunenud ja millised on selle rakenduslikud aspektid digitaalse kultuuripärandi säilitamisel. Artikkel keskendub küsimustele, milliseid omadusi peetakse tänapäeval määravaks digiobjekti autentsuse hindamisel ning milliseid strateegiaid ja institutsionaalseid praktikaid on rakendatud nende omaduste tagamiseks. Esmalt käsitletakse autentsuse teoreetilisi ja ajaloolisi lähtekohti ning normatiivset raamistikku, seejärel analüüsitakse digiobjekti objektiomaseid ja kontekstipõhiseid tunnuseid, sealhulgas olulisi omadusi ning nende seost säilitamisstrateegiatega. Viimaks vaadeldakse probleeme, mis tekivad digiarhiivides kultuuripärandi autentsuse hindamisel ja tagamisel, pidades silmas, et tegemist ei ole üksnes tehnilise, vaid ka organisatsioonilise, kultuurilise ja epistemoloogilise küsimusega.

Autentsuse teoreetilised ja normatiivsed käsitlused

Autentsus on sotsiaalselt konstrueeritud ja seega pidevas muutumises, nagu teisedki väärtushinnangud.[3] Antiikmaailmas ja varakeskajal seostati autentsust ennekõike autorluse ja legitiimsuse küsimusega. Tekstide ehtsust määratleti sageli nende väidetava apostelliku või autoriteetse päritolu kaudu, näiteks piiblikaanonites või hagiograafilistes allikates. Reliikviate ja liturgiliste objektide autentsus ei tulenenud mitte niivõrd nende materjalist või päritolust, kui nende seotusest jumaliku või pühaks peetud narratiiviga. Renessansiajastul ja varauusajal tõusis esile originaalsuse ideaal. Kunsti ja käsikirjade maailmas muutus oluliseks individuaalne autorlus

[3] Heather McNeil, Bonnie Mak, "Constructions of Authenticity", *Library Trends*, 56:1 (2007), 26–52.

ning autentsuse kandjateks said originaalobjekti füüsiline käsitlus, autori käekiri, materjalid ja kontekstilised tunnused.

Trükitehnoloogia areng tõi kaasa vajaduse määratleda paljundatava objekti autentne versioon. Valgustusajastul, mil kujunes klassikaline arhiivindus (18.–19. saj), formuleeriti autentsuse mõiste institutsionaalses võtmes. Briti ja Saksa arhiivinduses hakati autentsust defineerima, tuginedes objekti provenientsile ja algse korra austamise põhimõttele. Autentsus ei olnud enam pelgalt objektipõhine, vaid see seostati kogu säilitussüsteemi loogikaga.[4] Tuntud briti arhivaar ja arhiivindusteoreetik Sir Hilary Jenkinson (1882–1961) arvas, et arhiividokumentide autentsust kinnitab nende ametlik säilitamine.[5] 20. sajandi esimeses pooles, eriti seoses õigusteaduse ja diplomaatika arenguga, hakati rõhutama dokumentide autentsuse formaalseid kriteeriume, näiteks protokollilist järjepidevust, allkirja, pitserit ja käsikirjalisi tunnuseid.[6] Nii tõdes arhiiviteadlane Michael Cook: "Me ei usu enam, nii nagu Jenkinson uskus, et arhiivi väärtus uurimistöös või selle väärtus juriidilise tõendina sõltub meie kindlast teadmisest, et see pole kunagi asunud väljaspool ametlikku haldussüsteemi."[7]

Seniseid autentsuse ja usaldusväärsuse käsitlusi hakkas üha enam mõjutama digitaalse informatsiooni ulatuslik levik ja digiobjektide säilitamisega seotud probleemid. Esimesed 1969. aastal Ameerika rahvusarhiivi vastu võetud digidokumendid kujutasid endast lameandmebaase ja ASCII-vormingus tekstidokumente, millede autentsust hinnati lihtsalt väljaprintide visuaalse vaatlusega.[8] Seega käsitleti digidokumente esialgu sarnaselt paberkandjal olevate dokumentidega.[9] Digidokumentide autentsusega seotud probleemid tõusid esile 1990. aastate alguses. Ilmnes, et traditsioonilised autentsuse eeldused, nagu dokumentide füüsiline puutumatus või

---

4 Hilary Jenkinson, *A Manual of Archive Administration* (Oxford: Clarendon Press, 1922); Theodore R. Schellenberg, *Modern Archives Principles and Techniques* (Chicago: The University of Chicago Press, 1956).

5 Hilary Jenkinson, *A Manual of Archive Administration*. New and Revised (London: Percy Lund, Humphries & Co., 1937), 4. http://www.archive.org/details/manualofarchiveaooiljenk.

6 Harry Bresslau, *Handbuch der Urkundenlehre für Deutschland und Italien* (Leipzig: Verlag von Veit & Comp., 1915); Arthur Giry, *Manuel de diplomatique* (Paris: Librairie Felix Alkan, 1925).

7 Michael Cook, *The Management of Information from Archives* (Aldershot, Brookfield: Gower, 1986), 7, 129.

8 National Archives and Records Administration, *The History of the Electronic Records and ERA* (College Park: National Archives: Electronic Records Archives, 2015). http://www.archives.gov/era/about/history.html.

9 Vt lähemalt Konsa Kurmo, "Kuidas paberi kõrval hakati bitte ja baite säilitama? Digitaalse info säilitamise arengujooni", *Ajalooline Ajakiri*, 4 (2014), 359–378.

käsitsi kirjutatud allkirjad, ei kehti failipõhiste ja dünaamiliste objektide kohta. Digitaalses keskkonnas saab dokumenti muuta märkamatult, selle päritolu varjata ning koopiaid luua lõputul hulgal, ilma et nende visuaalne vorm muutuks. See kutsus esile vajaduse autentsuse teoreetiliseks ümbermõtestamiseks – kuigi traditsioonilised määratlused jäid oma põhiolemuselt samasteks, vajasid need täiendamist ja kontekstualiseerimist.

Digiobjektide autentsusega seotud küsimusi hakati tõsisemalt arutama alates 1990. aastate esimesest poolest.[10] 1993. aastal alustas Rahvusvahelise Arhiivinõukogu (The International Council on Archives, ICA) elektrooniliste dokumentide komitee projektiga, mille eesmärk oli teha uurimistööd, vahetada kogemusi ning koostada standardeid ja direktiive elektrooniliste dokumentide loomise ja arhiveerimise kohta. Ettevõtmise raames koostati kolm juhendmaterjali, kus käsitleti üsna põhjalikult ka digitaalsete dokumentide autentsust ja usaldatavust (*reliability*).[11] ICA juhendites rõhutati, et dokumente luues ja hoides on organisatsioonide peamine eesmärk tegevuste ja tehingute tõendamine, mille tagamiseks peavad digidokumendid olema loodud usaldusväärsetena (*reliable*) ja säilitatud autentsetena.[12] Need põhimõtted kehtivad ka praegu.

2000. aastal avaldas USA Raamatukogu- ja inforessursside nõukogu (The Council on Library and Information Resources, CLIR) aruande digiobjektide autentsuse kohta. Selle eesmärgiks oli koondada erinevate valdkondade (raamatukogundus, arhiivindus, arvutiteadus) seisukohad autentsusega seotud põhimõistete ja -terminite osas. Aruandes määratleti täpsemalt järgmised terminid: digiobjektide sisu (*content*), muutumatus (*fixity*), seoste kooskõla (*consistency of reference*), päritolu (*provenance*)

[10] Luciana Duranti, Terry Eastwood, "Protecting electronic evidence: a progress report on a research study and its methodology", *Archivi and Computer*, 3 (1995), 213–250; Wendy Duff, "Ensuring the preservation of reliable evidence: a research project funded by the NHPRC", *Archivaria*, 42 (1996), 28–45; Luciana Duranti, Heather MacNeil, "The protection of the integrity of electronic records: an overview of the UBC-MAS research project", *Archivaria*, 42 (1997), 46–67; David Bearman, Jennifer Trant, "Authenticity of Digital Resources: Towards a Statement of Requirements in the Research Process", *D-Lib Magazine*, 6 (1998), http://www.dlib.org/dlib/june98/06bearman.html.

[11] Alf Erlandsson, *Electronic Records Management: A Literature Review*. ICA Studies/Études CIA (Paris: International Council on Archives, 1996).

[12] Committee on Electronic Records, *Guide for Managing Electronic Records from an Archival Perspective* (Paris: International Council on Archives, 1997), 24.

ja kontekst (*context*).[13] Aruandes rõhutati tervikluse (*integrity*) tähtsust autentsuse määratlemisel digitaalsetes keskkondades.[14]

Esimene süsteemne autentsuse teoreetiline ümbermõtestamine toimus rahvusvahelise teadusprojekti InterPARES (International Research on Permanent Authentic Records in Electronic Systems) raames. 1999.–2018. aastal kestnud projektil oli neli etappi. Projekti esimeses etapis (1999–2006) määratleti püsivalt autentsete digitaalsete dokumentide säilitamise põhimõtted ja töötati välja autentsuse nõuded ja meetodid, millega hinnata, kas digitaalsed arhivaalid on säilitanud oma ehtsuse. Väljatöötatud autentsuse mudel ei eelda objekti materiaalse kuju püsivust, vaid selle funktsionaalset järjepidevust ja tõendatavust. Autentsus ei ole seega püsiv omadus, vaid institutsionaalselt hallatav ja dokumenteeritav seisund.[15] Selle mõtteviisi muutuse olulisim tagajärg oli nihe autentsuse käsitlemisel: varsemalt eeldati, et teatud institutsioonides (arhiivis, raamatukogus jms) säilitatavad objektid on autentsed, kuid siis tõdeti, et digitaalses arhiivinduses tuleb autentsust aktiivselt tõestada ja säilitada.

Euroopa kontekstis on oluline DLM Forum (Document Lifecycle Management Forum) ning selle organisatsiooni poolt välja töötatud MoReq (Model Requirements for Electronic Records Management) spetsifikatsioonid. MoReq (2001, uuendatud MoReq2 2008 ja MoReq2010) spetsifikatsioonid seadsid standardiseeritud nõuded digitaalsete dokumentide haldussüsteemidele, sh autentsuse tagamise funktsionaalsused.

20. sajandi lõpus toimunud postmodernistlik pööre muutis autentsuse käsitlust radikaalselt. Michel Foucault ja Jacques Derrida tõstatasid küsimusi arhiivi kui võimuinstrumendi ja kultuurimälu konstruktsiooni kohta.[16] Autentsus muutus tähenduslikuks – see polnud enam objekti omadus, vaid tõlgendamise tulemus. Eriti kultuuripärandi valdkonnas tõusis esile nn semantiline autentsus, mis hindab objekti tähenduslikku sobivust kasutaja, kogukonna või narratiivse konteksti suhtes.[17]

---

[13] *Authenticity in a Digital Environment* (Washington, D.C.: Council on Library and Information Resources, 2000), vi.

[14] Clifford Lynch, "Authenticity and Integrity in the Digital Environment: An Exploratory Analysis of the Central Role of Trust", *Authenticity in a Digital Environment* (Washington, D.C.: Council on Library and Information Resources, 2000), 32–50 (41). http://www.clir.org/pubs/reports/pub92/lynch.html.

[15] InterPARES Project, *The Long-Term Preservation of Authentic Electronic Records: Findings of the InterPARES Project* (Vancouver: University of British Columbia, 2006), 14–21.

[16] Michel Foucault, *The Archaeology of Knowledge* (London, New York: Routledge, 2012), 142–148; Jacques Derrida, *Mal d'archive: Une impression freudienne* (Paris: Galilée, 1995).

[17] Barbara Kirshenblatt-Gimblett, "Theorizing Heritage", Ethnomusicology 39:3 (1995), 367–380; Terry Cook, "Archival Science and Postmodernism: New Formulations for Old

Digiobjektide autentsuse tagamise küsimused on olulised digitaalkriminalistikas (*digital forensics*), mille meetodeid ja teoreetilisi põhimõtteid on hakatud rakendama ka arhiivinduses.[18] Võrreldes arhiivindusega käsitleb digitaalkriminalistika digiobjektide terviklust märksa detailsemalt, näiteks eristatakse nii loogilisel kui füüsilisel tasemel bitivoo, andmete ja arvutisüsteemi terviklust.[19]

Digiobjektid ja nende säilitamine

Digitaalse info säilitamisel on oluline mõista, kuidas digiobjekt tekib ja muutub kasutajale arusaadavaks. Selleks eristatakse kolme tasandit: füüsiline, loogiline ja kontseptuaalne.[20] Füüsiline tasand viitab andmekandjale, näiteks kõvakettale või mälukaardile, millele on salvestatud elektrilised signaalid. Kui sobiv riistvara neid signaale loeb, tõlgendatakse need tarkvara abil struktureeritud andmeteks, mida nimetatakse loogiliseks objektiks. Loogiline objekt on sellest kandjast sõltumatu, kindla failivormingu reeglite järgi struktureeritud bitijada. Objekti nimetatakse "loogiliseks" kuna tema identiteedi määrab loogika (süntaks), mille järgi tarkvara saab bitijada üheselt esitada. Loogiline objekt ei ole digiobjekti algne olemus, vaid pigem vahepealne struktuur, mis võimaldab andmeid töödelda ja esitada. Loogilisus tuleneb sellest, et objekt on masinloetav ja tarkvaraliselt interpreteeritav.

Tarkvara vahendusel muudetakse loogiline objekt inimesele või süsteemile arusaadavaks kontseptuaalseks objektiks, näiteks digitaalseks raamatuks, fotoks või lepinguks. Kontseptuaalne objekt on see, kuidas

---

Concepts", *Archival Science*, 1 (2001), 3–24; Tom Nesmith, "Seeing Archives: Postmodernism and the Changing Intellectual Place of Archives", *American Archivist*, 65:1 (2002), 24–41; Terry Cook, "Evidence, Memory, Identity, and Community: Four Shifting Archival Paradigms", *Archival Science*, 13:2-3, (2013), 95–120. Doi:10.1007/s10502-012-9180-7.

18 Luciana Duranti, "From Digital Diplomatics to Digital Records Forensics", *Archivaria*, 68 (2009), 39–66; Matthew G. Kirschenbaum, Richard Ovenden, Gabriela Redwine, Rachel Donahue, *Digital Forensics in Born Digital Cultural Heritage Collections* (Washington, D.C.: Council on Library and Information Resources, 2010); Jeremy Leighton John, *Digital Forensics and Preservation* (Great Britain: Digital Preservation Coalition and Jeremy Leighton John: Charles Beagrie Ltd., 2012. http://www.dpconline.org/component/docman/doc_download/810-dpctw12-03pdf.

19 Brian Carrier, "Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers", *International Journal of Digital Evidence*, 1:4 (2003), 1–12.

20 Kenneth Thioboedeau, "Overview of Technological Approaches to Digital Preservation and Challenges in Coming Years", *The State of Digital Preservation: An International Perspective* (Washington, D.C.: Council on Library and Information Resources, 2002), 4–31. https://www.clir.org/pubs/reports/pub107/.

kasutaja kogeb infoobjekti, sõltumata selle tehnilisest esitusviisist. Sama kontseptuaalne objekt võib olla esitatud mitmel erineval loogilisel kujul (nt tekstifailina või pildina), mis kõik vahendavad sama tähendust. Seega on digiobjekt kihiline, füüsiline kandja võimaldab loogilist struktuuri, mis omakorda vahendab kontseptuaalset tähendust. Autentsuse tagamisel tuleb arvestada kõigi nende tasandite seoseid ja muutusi.

Kontseptuaalse objekti sisu ja struktuur sisalduvad loogilises objektis või objektide kogumis, kuid sama kontseptuaalne tähendus võib olla esitatud erinevate loogiliste objektide kaudu. Näiteks võib ühe ja sama dokumendi sisu olla digitaalselt kodeeritud kas pildifailina (nt skaneeritud PDF) või tekstifailina (nt .docx või .txt). Kuigi mõlemad esitavad sama teksti, erinevad nad oluliselt oma struktuuri, kasutatavuse ja säilitamise nõuete poolest. See näide toob esile kaks digiobjektide autentsuse seisukohalt olulist eripära.

Esiteks, ühel kontseptuaalsel objektil võib olla mitu loogilist esitust, mis kõik säilitavad selle tähenduslikke tunnuseid, kuid mitte tingimata võrdselt. Näiteks pildiraamatu puhul ei pruugi .txt-fail säilitada illustratsioonide ja kujunduse kaudu edastatavat tähendust, samas kui EPUB või PDF võivad seda teha. Seetõttu tuleb säilitamisel määratleda, millised tunnused on konkreetses kontekstis olulised ja milline loogiline esitustase neid kõige paremini kannab.

Teiseks, digiobjekti säilitamiseks peab olema võimalik identifitseerida ja taastada kõik selle digitaalsed komponendid, nii füüsilised kui loogilised objektid, mis on vajalikud kontseptuaalse objekti esitamiseks. Need komponendid ei piirdu ainult sisutekstiga, vaid hõlmavad ka struktuuri- ja esituselemente, nagu lehekülje paigutus, kujundus, interaktiivsed funktsioonid või metaandmed. Näiteks interaktiivne veebileht võib sisaldada HTML-koodi, CSS-stiile, JavaScripti ja pilte. Tegemist on terve rea loogiliste objektidega, mis koos võimaldavad kontseptuaalse objekti, näiteks artikli või virtuaalnäituse korrektse esituse.

Kontseptuaalse objekti eraldamine füüsilisest ja loogilisest objektist tähendab ka seda, et mitu füüsilist objekti võivad esitada ühte kontseptuaalset objekti. Digifotoaparaadiga tehtud pilti säilitatakse RAW-failivormingus, kuid kasutamiseks tehakse RAW-failist koopia JPG-failivormingus. Need failivormingud on füüsiliste ja loogiliste objektidena erinevad, kuid kujutavad ühte ja sedasama kontseptuaalset objekti. Seega on tegemist ühe infoobjekti manifestatsioonide ehk esitustega (*representations*).

Väga oluline on eristada digiobjekti erinevaid esitusi eri versioonidest. Kui esitus on digiobjekti tehnilise muudatuse tulemus, siis versioonid on sisuliselt erinevad ja kujutavad endast uusi kontseptuaalseid objekte. Kui

me RAW-failivormingus olevat pilti kuidagi muudame, näiteks pöörame seda ja seejärel teeme muudetud failist koopia JPG-vormingus, on tegemist erinevate versioonidega, kuna kujutist ennast on muudetud.

Digiobjektide autentsus

Digiinfo säilitamise määratlustes rõhutatakse, et säilitamine tähendab säilitatavate digiobjektide kasutatavuse, arusaadavuse ja autentsuse tagamist.[21] Seega on autentsuse tagamine säilitamise üks esmaseid ülesandeid ja see ei ole seotud ainult digiobjektidega.

Tavakäsitluses mõistetakse autentsust sageli binaarselt – objekt on autentne või mitteautentne. Näiteks uurides Picassole omistatud maali, püüame kindlaks teha, kas teos on tõepoolest Picasso enda maalitud. Kui see nii on, loetakse maal autentseks. Kui teos on kellegi teise loodud, kuid esitatakse ehtsa Picasso maalina, siis on tegemist võltsinguga ehk mitteautentse objektiga. Siiski võib mõistet "autentsus" kasutada ka laiemas tähenduses. Kui teame, et tegu on Picasso teose jäljendusega, näiteks hariduslikul eesmärgil loodud koopiaga või muuks teadlikuks eksponeerimiseks loodud koopiaga, siis võib seda nimetada autentseks võltsinguks. See tähendab, et objekt ei püüa olla midagi muud kui see on – võltsing, mille identiteet ja päritolu on selgelt määratletud. Autentsus seisneb sel juhul objekti läbipaistvas esituses ja konteksti täpses dokumenteerimises.[22]

Kultuuripärandi valdkonnas leidub mitmeid näiteid, kus autentsus ei tähenda tingimata originaalsust, vaid usaldusväärset esitust. Mitmetes Euroopa linnades taastati hävinud hooned pärast Teist maailmasõda, näiteks Varssavi kuningaloss, Saksamaal Hildesheimi linna renessanss-stiilis turuplatsi hoonestus ja Dresdeni Frauenkirche. Tegemist ei ole originaalsete hoonetega, vaid autentsete rekonstruktsioonidega, st need põhinevad arhitektuurilistel uuringutel ja need on selgelt märgistatud kui rekonstruktsioonid. Juhul kui rahvariided või käsitööesemed taasluuakse traditsioonilisel viisil, tekib olukord, kus objekt ei ole ajalooline originaal, kuid on autentne oma valmistamisviisi ja kultuurilise tähenduse poolest. Sellest lähtuvalt võib autentsust määratleda kui objekti vastavust tema deklareeritud olemusele – autentne on see, mille identiteet ja päritolu on tuvastatavad ning kooskõlas sellega, mida objekt väidab end olevat. Kultuuripärandi

[21] Kurmo Konsa, *Bitid purki: teabe säilitamine digiühiskonnas* (Tartu: Kõrgem Kunstikool Pallas, 2018), 30–32.

[22] Luciana Duranti, *Diplomatics: new uses for an old science* (Lanham: Scarecrow Press, 1998), 46.

kontekstis tähendab see sageli tähendusliku ja läbipaistva esituse tagamist, mitte originaalsuse kinnitamist.

Dokumendihalduses ja arhiivinduses käsitletakse autentsetena dokumente, mille puhul saab kindlaks teha, et dokument on just see, mis see on mõeldud olema. Dokumendi loojaks või saatjaks on isik, kes pidi selle looma või saatma ning dokument on loodud või saadetud ajal, mil see pidi loodama või saadetama.[23] Teiseks oluliseks autentsusega seotud mõisteks on usaldusväärsus (*reliability*), tähendab, et objekti sisu või info, mida ta edastab, on täpne, täielik ja usaldatav. Kui vaadata eelpooltoodud Picasso maali näidet, siis see, kas autentne Picasso võltsing on usaldusväärne, sõltub sellest, millena seda objekti meile esitatakse. Kui võltsing esitatakse ehtsa Picassona, siis see ei ole usaldusväärne, kuna sisu (s.t väide, et see on Picasso) ei vasta tõele. Kui võltsing esitatakse võltsinguna, siis see on usaldusväärne, kuna väide (et tegemist on võltsinguga) vastab tõele.

Arhiivinduses on dokumendi usaldusväärsus seotud selle sisuga: usaldusväärne on dokument, mille sisu võib pidada täpseks, täielikuks ja tõendatavaks esituseks toimingutest, tegevustest või faktidest. Autentsus seevastu viitab dokumendi identiteedi ja päritolu tuvastatavusele ning sellele, et dokument on see, millena ta end esitab. Seega, kui dokument on autentne, kuid sisaldab valeinfot, näiteks ekslikke mõõteandmeid, ei saa seda pidada usaldusväärseks. Samas võib võltsitud dokument olla sisult täpne, näiteks sisaldada korrektselt esitatud sündmuste kirjeldust, kuid autentsuse puudumise tõttu ei saa seda üldjuhul kasutada tõendusmaterjalina. Erandiks on olukorrad, kus dokumenti kasutatakse just võltsimise tõendamiseks, näiteks juhul, kui soovitakse näidata, et dokument on sihilikult muudetud või esitatud eksitaval viisil. Sellisel juhul võib võltsitud dokument ise olla tõendiks võltsimise fakti kohta, mitte aga tõendavaks allikaks dokumenteeritud sündmuse kohta.

Digiobjektide autentsuse määratlemiseks on välja töötatud mitmeid rahvusvaheliselt tunnustatud käsitlusi, mis toovad välja erinevaid, kuid omavahel seotud aspekte. Need käsitlused aitavad mõista, et autentsus ei ole üheselt määratletav omadus, vaid mitmetasandiline kvaliteet, mis sõltub kontekstist, kasutusest ja institutsionaalsest raamistikust.

Üks täpsemaid määratlusi on loodud InterPARES projekti raames: digitaalne dokument loetakse autentseks juhul, kui (1) tema identsus (autor, loomise aeg, seotus tegevustega) on usaldusväärselt tuvastatav ja (2) tema terviklus (sisu, struktuur ja kontekstitunnused) on säilinud või

[23] EVS-ISO 15489-1:2017 Informatsioon ja dokumentatsioon. Dokumendihaldus. Osa 1: Mõisted ja põhimõtted, 2017.

dokumenteeritult muutunud. See määratlus rõhutab, et autentsus ei seisne pelgalt faili muutumatuses, vaid selle dokumenteeritud elutsüklis ja konteksti säilimises.[24]

Sarnast põhimõtet väljendab UNESCO määratlus, mille kohaselt on autentsus digiobjektide omadus olla "need, mis nad on mõeldud olema". See kehtib nii originaalsete objektide kui ka nende usaldusväärsete koopiate kohta tingimusel, et koopiate loomise protsess on täielikult dokumenteeritud. See määratlus rõhutab autentsuse seotust digiobjekti säilitamise ja taasesitamise protsessi läbipaistvusega.[25]

ISO standard 15489 toob autentsuse määratlusse sisse institutsionaalse ja halduslikku mõõtme. Autentne dokument on see, mis "on loodud või saadud õiges kontekstis, õigel ajal ja õigel viisil ning on säilinud muutmatuna või dokumenteeritud muutustega". Lisaks seostatakse autentsust teiste arhiivinduslike põhiomadustega, nagu usaldusväärsus, terviklus ja kasutatavus, rõhutades, et dokumentide halduse süsteemid peavad tagama nende omaduste säilimise läbi aja.[26]

Avatud arhiiviinfosüsteemi mudel (OAIS[27]) lisab autentsuse käsitlusse hinnangulisuse aspekti. OAIS määratleb autentsuse kui määra, mille puhul inimene või süsteem võib pidada objekti selleks, mis ta on mõeldud olema. Autentsuse määra hinnatakse tõendite (*evidence*) alusel, mis tähendab, et autentsus ei ole absoluutne, vaid sõltub objekti kohta kättesaadavast ja usaldatavast informatsioonist.[28]

Kokkuvõttes näeme, et kuigi erinevad määratlused kasutavad erinevat keelt ja rõhuasetusi, on tegemist sarnase arusaamaga, mille kohaselt autentsus tähendab digitaalses kontekstis objekti identiteedi, tervikluse ja konteksti usaldusväärset tuvastatavust. Autentsuse tuvastamine nõuab lisaks tehnilisele kontrollile ka institutsionaalset vastutust ja dokumenteeritud säilitusahelat.

---

[24] InterPARES Project, *The Long-Term Preservation of Authentic Electronic Records: Findings of the InterPARES Project* (Vancouver: University of British Columbia, 2006), 14–21.

[25] National Library of Australia, *Guidelines for the preservation of digital heritage* (UNESCO, 2003), https://unesdoc.unesco.org/ark:/48223/pf0000130071.

[26] International Organization for Standardization, ISO 15489-1:2016 – Information and documentation – Records management – Part 1: Concepts and principles (Geneva: ISO, 2016), §3.15.

[27] Digitaalse ainese arhiiviinfosüsteemide funktsionaalne standardmudel (ingl) Open Archival Information System.

[28] *Recommendation for Space Data System Practices. Reference model for an open archival information system (OAIS)* (Washington: The Consultative Committee for Space Data Systems, 2012), 19. https://public.ccsds.org/pubs/650x0m2.pdf.

Autentsuse kontseptualiseerimisel digitaalkeskkonnas on oluline roll ka metaandmete standarditel, nagu PREMIS (Preservation Metadata: Implementation Strategies). PREMIS eristab autentsuse tõendamiseks nelja põhivaldkonda: objekti identifikaatorid, tegevuste logid (nt migratsioonid, valideerimised), provenientsi ahel ning kasutusõiguste ajalugu.[29] Neid elemente käsitletakse mitte üksnes dokumentide kohta käiva infona, vaid kui autentsust tagavate toimingute osa – metaandmed ei kirjelda ainult objekti, vaid loovad ja hoiavad selle autentsust.[30]

Eeltoodud autentsuse määratlusi analüüsides on näha, et autentsus tuleneb digiobjektide korral nende järgmistest tunnustest:

- identsus (*identity*);
- terviklus (*integrity*);
- kasutatavus (*usability*).

Identsus tähendab, et objekt on just see, mis ta peaks olema ja teda ei aeta segi mõne teise objektiga. Identsus digitaalses kontekstis tähendab seda, et objekti saab üheselt määratleda ja eristada teistest objektidest, olgu need väliselt sarnased koopiad, erinevad versioonid või seotud dokumendid. Identsus on küllaltki lai mõiste, viidates suurele hulgale tunnustele, mis kõik aitavad seda identifitseerida kui unikaalset, kõikidest teistest objektidest eristuvat objekti. Tegemist on omaduste kogumiga, mis võimaldavad objekti identifitseerida, mõista ja eristada. Toome järgnevalt ülevaate nendest omadustest.

Sisu (*content*) on objekti infot kandev osa, mille võivad moodustada tekstid, kujutised, arvutikood jm. Tegemist on objekti semantilise või funktsionaalse sisuga, kuid oluline täiendus on, et sisu on eristatav selle esitlusest ja struktuurist. Näiteks HTML-faili sisu on kood ise, esitlus on see, mida brauser näitab. Sisu ei pea tingimata olema inimestele loetav, vaid võib olla arusaadav ainult teistele arvutisüsteemidele.

Välimus (*look*) tähendab seda, kuidas sisu on nähtav sellega interakteeruvale agendile, olgu selleks siis inimene või teine arvutisüsteem. Tekstide puhul on näiteks olulised kasutatud kirjatüüp, kirja suurus, värvus, kujundus jm. Oluline on märkida, et esitusviis võib mõjutada tähendust, eriti kultuuripärandi kontekstis. Näiteks sama tekst erineva kirjatüübiga võib kanda eri esteetilist või kontekstuaalset tähendust.

---

[29] Library of Congress, *Understanding PREMIS, Version 3.0* (Washington D.C., 2015), 17–25.

[30] Library of Congress, *Understanding PREMIS, Version 3.0* (Washington D.C., 2015), 28.

Kontekst (*context*) tähendab taustinfot, mis aitab mõista digiobjekti tehnilisi ja sotsiaalseid seoseid, ja objekti päritolu (info looja ning hilisemad muutused selle omanike ja haldajate hulgas). Lühidalt öelduna tähendab kontekst seda, kes, millal ja miks on selle digiobjekti loonud. Kontekst hõlmab seega nii loomiskonteksti, kui ka halduse ja kasutamise konteksti (kes objekti kasutavad ja säilitavad, millal seda muudeti või kasutati) ja seoseid teiste objektidega (kas see on näiteks sarja osa, kas see on seotud teiste failidega). Konteksti aspekt on eriti oluline autentsuse tuvastamisel, sest ilma kontekstita ei saa kindlaks teha identiteeti ega päritolu.

Struktuur (*structure*) kirjeldab objekti sisu moodustavate osade (manusfailid, leheküljed, muud eraldiolevad tekstiosad jne) asetust ja omavahelist seost. Digiobjektides on eriti oluline struktuur, et säiliks tähendus ja funktsioon. Struktuur on ka kasutatavuse eelduseks, kui see on rikutud, võib objekt muutuda mõistetamatuks.

Käitumine (*behaviour*) on seotud objektile omase funktsionaalsusega. See viitab objektide interaktiivsetele või dünaamilistele omadustele (hüpertekstilingid, ajakohastuvad arvutused, aktiivsed lingid jms), mida sageli eiratakse. Digitaalse säilitamise kontekstis tähendab see seda, et käitumise säilitamiseks tuleb mõnikord talletada ka tarkvarakeskkond või selle emulatsioon.

Lisaks objekti enda kontseptuaalsele struktuurile on identsus seotud laiema õigusliku, sotsiaalse ja tehnoloogilise kontekstiga. OAIS mudelis on objekti identsuse kirjeldus seotud säilituskirjeldusinfoga (*preservation description information*, PDI), mis aitab mõista digiobjekti laiemat keskkonda. Digiobjekti identsuse käsitlemisel tuleb seda vaadelda mitte isoleeritud objektina, vaid lahutamatus seoses kontekstiga. Digiobjekti näol on tegemist teistest eristuva objektiga, millele annavad tähenduse seosed kontekstiga. Kuna objekti kontekst ja tema seosed sellega muutuvad pidevalt, siis on vajalik nende pidev dokumenteerimine, et objekti autentsus ei kahjustuks.

Terviklus (*integrity*) viitab sellele, et objekt on säilitatud muutumatul kujul või kõik tehtud muutused on jälgitavad ja ei ole kahjustanud objekti identsust. Kujutlegem näiteks, et meil on digiobjekt, mis koosneb kolmest osast, kuid me ei tea, et neid osasid peab kolm olema. Avastame oma repositooriumist ainult kaks osa ja eeldame ekslikult, et see ongi terviklik objekt. Kontrollime need kaks osa üle ja leiame, et need on tehniliselt autentsed ja usaldusväärsed. Kuna tegemist ei ole siiski tervikliku ressursiga, ei saa me seda ikkagi käsitada täielikult autentsena. Samas ei tähenda terviklus seda, et objekt ei ole üldse muutunud. Kõik säilitatavad objektid muutuvad ajas: füüsiliste objektide materjalid lagunevad ja kahjustuvad, keemilised

ja füüsikalised omadused muutuvad. Digiobjektide muutused võivad tuleneda andmekandjate vahetusest, failivormingu muutmisest või säilitustehnoloogia uuendamisest, kuid sellised toimingud ei tohi muuta objekti identiteeti ega kahjustada selle tähendust. Seega on autentsuse säilitamisel keskne roll just sellel, et muutused on kontrollitud, dokumenteeritud ja eesmärgipärased. Terviklus on eriti aktuaalne komplekssüsteemide (nt andmebaaside, veebilehtede, audiovisuaalsete arhiivide) puhul, kus ressursi täielikkus sõltub mitmest omavahel seotud failist.

Kasutatavus (*usability*) tähendab, et infoobjekt on leitav, kättesaadav, esitatav ja mõistetav nii praeguses kui ka tulevases kasutuskontekstis. Selleks peab olema tagatud, et objektil on piisavad metaandmed, et see oleks otsitav ja leitav (*retrieve*), objekti saab kasutaja või arvutisüsteem avada, et selle sisule ligi pääseda (*access*), arvestades ligipääsuõigusi ja tehnilisi piiranguid. Oluline on, et objekti saab korrektselt esitada (*present*) ning kasutaja või infosüsteem suudab objekti tõlgendada (*interpret*), tuginedes vajalikule abiteabele, dokumentatsioonile või konteksti infole. Lõppkasutaja peab saama vajaliku infoobjekti kätte ja olema võimeline seda ka mõistma. Kasutatavus on autentsuse seisukohalt oluline, sest ilma selleta ei ole võimalik objekti tuvastada, verifitseerida ega selle tähendust mõista.

Autentsuse olulisus digiobjektide korral

Infoobjektide põhimõttelised tunnused (identiteet, terviklus ja kasutatavus) sobivad autentsuse iseloomustamiseks nii digitaalse kui ka mittedigitaalse info korral. Seega on erineval kujul esinevate infoobjektide autentsuse käsitlus põhimõtteliselt ühesugune. Küll on aga nende tunnuste tagamise, kontrollimise viisid ja tööriistad erinevad, sõltudes sellest, milliste objektidega on tegemist. Kuna digiobjektid on oma olemuselt kergesti muudetavad ning nende muutmist on sageli raske tuvastada, on ka nende autentsuse tagamine märksa keerukam võrreldes traditsiooniliste infokandjatega.

Digitaalse info säilitamisel ja kasutamisel tehakse sageli mitmeid vajalikke muudatusi, nagu vormingu konversioonid, platvormi- või tarkvaravahetused, andmekandjate migreerimine. Kõik need võivad mõjutada objekti terviklust ja esitusviisi ning seada kahtluse alla selle autentsuse. Erinevalt paberdokumentidest, mille füüsilist muutmist on küllatki keeruline varjata, võib digiobjekti muuta nii, et muudatusest ei jää mingit jälge, kui neid ei logita ega kontrollita. Lisaks võivad digiobjektist eksisteerida mitmed koopiad ja versioonid, millede eristamine ilma versioonihalduse ja metaandmeteta võib osutuda keerukaks.

Autentsuse hindamiseks tuleb teada objekti autorit, loomise aega, päritolu ja kõiki olulisi muutusi selle elutsükli jooksul. Kuid just need aspektid võivad digitaalses keskkonnas kaduda, olla ebatäpsed või raskesti rekonstrueeritavad. Seetõttu ei piisa autentsuse kontrolliks üksnes faili olemasolust, vaid vajalik on kogu säilitusahela dokumenteerimine ja kontrollitavus. See muudab autentsuse tagamise digikeskkonnas tunduvalt keerukamaks kui traditsiooniliste infokandjate autentsuse hoidmine ning nõuab teadlikku ja süsteemset lähenemist, mis hõlmab nii tehnilisi, korralduslikke kui ka juriidilisi meetmeid.

Kui me säilitame paberdokumente, kunstiteoseid või digitaalseid või muid objekte, siis ideaaljuhul ei tohiks nende säilitamise käigus midagi olulist muutuda. Tegelikkuses pole see aga täielikult võimalik ega ka tingimata vajalik. Isegi paberil kirjalikud dokumendid ei ole täielikult püsivad, kuna paberi keemiline koostis, tindi värvus ja materjalide struktuur muutuvad aja jooksul. Need muutused on enamasti aeglased ja kergemini jälgitavad, sest sisu ja kandja moodustavad ühe füüsilise terviku. Digiobjektide säilitamine erineb füüsilise objekti säilitamisest põhimõtteliselt, kuna ei säilitata objekti kui füüsilist üksust, vaid tema võimet olla korrektselt esitatav ja mõistetav kindlas kontekstis. Digiobjekt taasesitatakse kasutajale, olgu selleks inimene või masin, arusaadaval kujul vastava tarkvara abil. See esitlus sõltub füüsilise andmekandja bititasandil talletatud andmete, failivormingu, metaandmete ja tarkvarakeskkonna koosmõjust. Kuigi lõppkasutaja ei näe ega mõista digiobjekti bititasandit, on selle täpsus ja terviklus autentsuse ja kasutatavuse tagamiseks hädavajalikud. Seega ei ole digisäilituse eesmärk üksnes failide säilitamine, vaid nende kasutatavuse ja usaldusväärsuse tagamine ajaga muutuvas tehnoloogilises keskkonnas.[31]

Traditsioonilises arhiivinduses peeti sageli autentsust, usaldusväärsust ja täpsust omavahel tihedalt seotud omadusteks. Digitaalse info korral ei ole aga objektide usaldusväärsus (*reliability*) ja täpsus (*accuracy*) enam vältimatult seotud autentsusega. Näiteks võib digiobjekt olla tehniliselt autentne, kuna selle päritolu ja säilitusahel on tuvastatavad, kuid sisaldada ebaõiget infot, nagu valed mõõteandmed või ekslikud kuupäevad. Samas võib objekt olla sisuliselt täpne ja usaldusväärne, kuid muudetud või migreeritud tundmatus keskkonnas, mistõttu pole selle autentsus enam kontrollitav. Oluline on rõhutada, et sama kehtib ka füüsiliste objektide puhul. Näiteks võib arhiivis säilitatav paberallikas või kunstiteos olla autentne, olles tõepoolest see, milleks seda peetakse, kuid samas sisaldada valeandmeid, eksitavat tõlgendust või propagandistlikku sisu. Sellisel juhul on

[31] Konsa, *Bitid purki: teabe säilitamine digiühiskonnas*, 30–32.

objekt autentne, kuid mitte usaldusväärne faktide esitamise seisukohalt. Autentsus, usaldusväärsus ja täpsus võivad olla omavahel kooskõlas, kuid võivad esineda ka sõltumatult. Samuti saab neid rikkuda kas ühiselt või eraldi, sõltuvalt objekti elutsüklist, säilituskeskkonnast ja kasutusviisist.[32]

Kultuuripärandi objektide kontekstis on järjest olulisem ka autentsuse kultuurilooline ja tähenduslik mõõde. Näiteks muuseumide digiarhiivides, virtuaalnäitustel või loovobjektide dokumentatsioonis ei pruugi autentsus seisneda üksnes vormilises vastavuses lähtekontekstile, vaid ka kuraatori, uurija või kogukonna tõlgenduses.[33] Autentsus omandab siin performatiivse mõõtme – see tekib taasesituse, kasutuse ja seostamise kaudu. See ei tähenda, et arhiivinduslik autentsus kaotab oma tähtsuse, vaid et digiobjekti autentsus võib olla kihtidena esinev nähtus, kus failitase, esitustase ja tähendustase võivad erineda, ent vajavad kõiki läbipaistvat haldamist.

Kokkuvõtlikult võib öelda, et digiobjektide autentsuse kaasaegne käsitlus tugineb formaalsele ja normatiivsele raamistikule, institutsionaalsele ja protsessipõhisele juhtimisele ning vajadusel ka tähendusloome ja konteksti arvestamisele, eriti kultuuripärandiga seotud objektide puhul.

Objektiomased ja kontekstipõhised autentsuse tunnused

Digitaalsete kultuuripärandi objektide autentsuse määramisel on kesksel kohal kaks omavahel tihedalt seotud, kuid analüütiliselt eristatavat kategooriat – objektiomased tunnused ja kontekstipõhised tunnused. Esimesed viitavad otseselt digiobjekti enda struktuurile ja sisule, kõigele sellele, mida saab digiobjektis tehniliselt mõõta, dokumenteerida ja võrrelda. Teised puudutavad aga objekti loomise, kasutamise ja säilitamise keskkonda, ehk seda, millised sotsiaalsed, institutsionaalsed ja semantilised seosed objekti raamivad.

Digitaalse autentsuse normatiivses raamistikus, nagu InterPARES ja PREMIS, eeldatakse, et objekti identiteet ja terviklus on mõistetavad just läbi nende kahe kategooria koosmõju. Ilma objektiomaste tunnusteta ei saa

---

[32] Luciana Duranti, "The long-term preservation of accurate and authentic digital data: the InterPARES Project", *Data Science Journal*, 4 (2005), 106–118; Duranti, MacNeil, "The protection of the integrity of electronic records", 48; Luciana Duranti, Ken Thibodeau, "The concept of record in interactive, experiential and dynamic environments: the view of InterPARES", *Archival Science*, 6:1 (2006), 13–68 (54); Heather MacNeil, Anne J. Gilliland-Swetland, "Authenticity task force report", *The long-term preservation of authentic electronic records: finding of the InterPARES Project*, toim Luciana Duranti (San Miniato: Archilab, 2005), 21.

[33] Fiona R. Cameron, "Object-oriented democracies: conceptualising museum collections in networks", *Museum Management and Curatorship*, 23:3 (2008), 229–243.

kinnitada, et dokument on säilinud terviklikuna ning ilma kontekstiinfota ei saa usaldusväärselt tuvastada, mis dokument see üldse on.

Objektiomased tunnused on digiobjekti omadused, mis on tuvastatavad ja tõendatavad selle bitijada, struktuuri ja sisuliste elementide kaudu. Sellisteks elementideks on näiteks failivorming ja struktuur, mis määravad ära selle, kuidas teave on organiseeritud ja millised tarkvaralised ressursid on selle kasutamiseks vajalikud. Failivorming ja struktuur on digiobjektide autentsuse seisukohalt kriitilise tähtsusega, sest need määravad, kuidas objekti saab identifitseerida, mõista, kasutada ja säilitada, ning hinnata, kas seda saab pidada samaks usaldusväärseks objektiks ka tulevikus. Kontrollsumma (*checksum*) on digitaalse objekti bititasandi tervikluse kontrollimise vahend. See on algoritmi abil arvutatud lühikood (nt SHA-256, MD5), mis tuletatakse faili sisust. Kui fail muutub, muutub koheselt ka kontrollsumma. Autentsuse seisukohalt on kontrollsummadel oluline, kuid piiratud roll. Need on vajalikud, aga mitte piisavad autentsuse tagamiseks. Versioonihaldusteave võimaldab jälgida, dokumenteerida ja hallata muudatusi, mis tehakse digitaalsele objektile selle elutsükli jooksul. Digiarhiivide kontekstis ei ole see pelgalt tehniline tööriist, vaid autentsuse haldamise kriitiline komponent, kuna see võimaldab tõendada, mida on muudetud, millal see toimus, kelle poolt ja miks seda tehti. Versioonihaldus loob auditijälje, mis tõendab, et muudatused tehti kontrollitud keskkonnas ja sihipäraselt. Digitaalallkiri ja ajatempel on kaks olulist mehhanismi, millega saab tugevdada digiobjekti autentsuse, päritolu ja tervikluse tõendatavust. Neid kasutatakse eelkõige õiguslikult või administratiivselt tundliku teabe korral, kuid ka kultuuripärandiga seotud digiarhiivides võivad need mängida olulist rolli, eriti säilitusahela alguses või digiarhiividevahelises andmevahetuses.

Autentsuse seisukohalt tuleb eristada neid omadusi, mille kadumine tähendab objekti autentsuse kaotust ja neid, mis on teisese tähtsusega. See eristus on sageli kontekstitundlik: mõne uurija või asutuse jaoks võib visuaalne kujundus olla määrav, teise jaoks piisab sisust ja kuupäevast.

Kontekstipõhised tunnused annavad vastuse järgmistele küsimustele: kust digiobjekt pärineb, miks see loodi ja kuidas see tekkis ning kuidas seda on käsitletud. Autentsuse seisukohalt on kontekst vähemalt sama oluline kui fail ise, kuna just konteksti kaudu saab määratleda objekti identiteedi ning hinnata, kas selle olemus on säilinud. Annan järgnevalt ülevaate olulisematest kontekstipõhistest tunnustest. Provenients annab teavet objekti looja, asutuse ja töökeskkonna kohta, milles see tekkis. Funktsionaalne kontekst viitab objekti seosele konkreetse tegevuse, menetluse või sündmusega. Arhiivinduslikult võib see hõlmata seost fondi või sarjaga.

Kasutusajalugu ja järelvalveahel (*chain of custody*) näitavad, kes ja millal on objektiga tegelenud, kuidas on seda muudetud ning kellele on see kuulunud. Metaandmed ja kirjeldavad andmestikud sisaldavad objekti identifitseerimist ja tähendust toetavat teavet (nt MuIS-is või FIS-is sisalduvad säiliku kirjed, valdkondlik klassifikatsioon, seotud märksõnad). Teave digiarhiivi või repositooriumi kohta, kus digiobjekte säilitatakse ja kasutatakse on eriti oluline raamatukogude ja muuseumide puhul. Digiarhiivi kontekst võib mõjutada objekti ligipääsetavust, käitumist ja tähendusvälju. Objekti tähendus võib sõltuda sellest, kuidas see on olnud seotud teiste objektide, narratiivide või eksponeerimispraktikatega.

Oluline on teadvustada, et kontekstipõhiseid tunnuseid ei saa pelgalt fikseerida, neid tuleb süstemaatiliselt hallata, versioonide kaupa talletada ning seostada iga säilitustoiminguga. Näiteks metaandmed, mis fikseerivad objekti migratsiooni ühest failiformaadist teise, peavad säilitama viite selle muutuse põhjusele, kuupäevale ja vastutavale osapoolele. Vastasel juhul ei saa tulevikus tõendada, et objekt on säilinud autentsena, isegi kui selle bittide kontrollsumma ei ole muutunud.

Objektiomased ja kontekstipõhised tunnused on omavahel tihedalt seotud. Faili bitijärjestus võib säilida, kuid kui selle kirjeldavad metaandmed kaovad või muutuvad vastuolulisteks, pole enam võimalik faili autentsust tõendada. Samuti ei piisa konteksti hoidmisest, kui digiobjekt migreerimisega on selle tähenduslikud omadused kaduma läinud.

Digiobjektide olulised omadused

Kuna digiobjekte kasutamise ja säilitamise käigus muudetakse, on kujunenud vajadus määratleda ja fikseerida digiobjekti olulised omadused (*significant properties*, *essential characteristics*, *essential elements*, *essence*), mis tuleb igal juhul säilitada. Digiobjekti oluliste tunnuste kontseptsioon formuleeriti esmakordselt CEDARS-projekti (1998–2002) käigus. Oluliste tunnustena käsitleti neid tehnilisi, intellektuaalseid ja esteetilisi tunnuseid, mis arhiivi või kogude kuraatori arvates tuleb kindlasti säilitada pika aja kestel.[34]

Hedstrom ja Lee mõistsid oluliste tunnuste all digiobjektide omadusi, mis mõjutavad nende kvaliteeti (*quality*), kasutatavust (*usalbility*), esitamist (*rendering*) ja käitumist (*behavior*). Neid omadusi võib grupeerida

[34] Gareth Knight, Maureen Pennock, "Data without meaning: establishing the significant properties of digital research", *The International Journal of Digital Curation*, 4:1 (2009), 159–174 (160). http://www.ijdc.net/index.php/ijdc/article/viewFile/110/87.

järgnevatesse kategooriatesse: sisu, kontekst (keskkond, kus objekt on loodud), välimus (nt kujundus, värvus), käitumine (nt interaktiivsus, funktsionaalsus) ja struktuur (nt leheküljed, lõigud).[35]

Mitu määratlust rõhutab, et objekti olulised omadused tuleb säilitada, et seda oleks võimalik tulevikus kasutada. Selline definitsioon on ka näiteks UNESCO-l: digiobjekti elemendid, tunnused ja omadused tuleb säilitada, et digiobjekti olulist tähendust saaks taasesitada või see saaks täita oma eesmärki.[36] Ka teine määratlus rõhutab, et digiobjektide tunnused tuleb säilitada, et tagada objektide kättesaadavus, kasutatavus, tähenduslikkus ja objektide võime olla tunnistus selle kohta, mida nad on määraletud kajastama.[37]

Seega kuulub digiobjekti oluliste omaduste hulka nii tehnilisi kui ka sotsiaalseid tunnuseid, kuid mitte kõik originaalobjekti omadused ei ole olulised. Oluline on silmas pidada konkreetse digiobjekti määratletud kasutajaskonda, kuna olulised omadused sõltuvad kasutajast ja kasutamise eesmärgist. Erinevate objektitüüpide ja kontekstide korral on need erinevad ja nende määratlemisel on vaja arvestada järgmiseid asjaolusid:

- säilitava institutsiooni eesmärgid;
- huvigruppide nõudmised;
- objekti tüüp;
- õiguslikud aspektid;
- institutsiooni võimekus.

Huvigrupid võivad olla erinevad ja moodustuvad digiobjekti praegustest ja tulevastest kasutajatest:

- digiobjekti looja, kes lõi objekti, näiteks avaldamiseks kirjutatud artikkel, Facebooki laetud foto, et täita suhteliselt lühiajaline spetsiifiline eesmärk;
- määratletud kasutajaskond, kes kasutab digiobjekti info hankimiseks, edasiseks uurimiseks jne;
- õpetajad ja õppejõud, kes kasutavad digiobjekti õpetamisel;

---

35 Margaret Hedstrom, Christopher A. Lee, "Significant properties of digital objects: definitions, applications, implications", *Proceedings of the DLM-Forum*, (2002), 218–227 (218). https://ils.unc.edu/callee/sigprops_dlm2002.pdf.

36 Guidelines for the preservation of digital heritage. Prepared by the National Library of Australia (Paris: UNESCO, 2003), 157–158. unesdoc.unesco.org/images/0013/001300/130071e.pdf.

37 Stephen Grace, Gareth Knight, Lynne Montague, *InSPECT final report* (London: King's College London, 2009), 3. www.significantproperties.org.uk/inspect-finalreport.pdf.

- institutsioon, kus soovitakse säilitada autentset objekti.[38]

Eri huvigruppide nõudmised digiobjekti funktsionaalsusele on erinevad ja need võivad aja jooksul muutuda. Digiobjekti olulised tunnused peavadki olema määratud lähtudes kasutajate vajadustest, mitte näiteks digiobjekti tehnilistest omadustest.[39] Objekte on erinevat tüüpi ja objekti looja võib valikul lähtuda nii oma eelistustest, kättesaadavast tarkvarast kui ka võimalikust auditooriumist, kellele objekt on suunatud. Näiteks ettekanne võib olla kirjutatud nii e-kirjana kui ka tekstidokumendina, kuid neil on ühised tunnused (tekst ja selle esitamise viis), kuid e-kiri nõuab täiendavaid omadusi kirja saaja fikseerimiseks.

Oluliste omaduste säilitamine võib olla õigusaktidega piiratud, mistõttu pole võimalik säilitada kõiki olulisi tunnuseid. Näiteks võib artikkel sisaldada teksti ja kujutisi, millede autoriõigus kuulub teksti loojale, aga artikli vorming ja tüpograafia kuulub väljaandjale ja neid ei või reprodutseerida. Oluliste omaduste säilitamine sõltub ka olemasolevatest rahalistest ja tehnilistest võimalustest.

Oluliste omaduste määratlemine on otsustava tähtsusega digiobjektide säilitusmeetodite valikul. Kui me teame, millised on need omadused, mis peavad säilitamise kestel alles jääma, siis saame valida ka vastavad meetodid. Välja on töötatud erinevate digiobjektide (nt struktureeritud tekstidokumendid, digitaalsed audiofailid, rasterkujutised, vektorkujutised, e-kirjad, videofailid, tarkvara, e-õpiobjektid, veebilehed) oluliste omaduste nimekirju. Need loetelud keskenduvad digiobjektide tehnilistele tunnustele, kuid nende tunnuste tähendus jääb harilikult täpsemalt määratlemata. See on aga kindlasti teave, mis peab sisalduma vastavas esitusinfos, et määratletud kasutaja suudaks taastada digiobjekti olulised omadused.[40] Digiobjekti olulised omadused on osaliselt seotud objekti autentsusega ja eriti selle püsimisega digiobjektide muutmisel.

OAIS mudelis otseselt digiobjektide olulistest omadusest juttu ei ole, selle asemel tuuakse sisse infotunnuse (*information property*) mõiste. Sõltuvalt kontekstist võib infotunnuse ja digiobjekti oluliste omaduste mõisted kattuda. Infotunnused on see osa sisuinfost, mida iseloomustatakse

---

38 Gareth Knight, Maureen Pennock, "Data without meaning: establishing the significant properties of digital research", *The International Journal of Digital Curation*, 4:1 (2009), 159–174 (162). http://www.ijdc.net/index.php/ijdc/article/viewFile/110/87.

39 Nick Del Pozo, Andrew Stawowczyk Long, David Pearson, ""Land of the lost": a discussion of what can be preserved through digital preservation", *Library Hi Tech*, 28:2 (2010), 290–300 (293).

40 David Giaretta, *Advanced digital preservation* (Berlin, Heidelberg: Springer, 2011), 217.

infotunnuse kirjelduses (*information property description*). Teatud osa sisuinfost, mis sisaldub sisuinfo objektis (*content data object*) ja selle esitusinfos, kirjeldatakse mingil spetsiifilisel põhjusel eraldi. Infotunnuste kirjeldused on olulised, kui digiobjekte migreeritakse. OAIS soovitabki määratleda transformatsioonilise infotunnuse (*transformational information property*). Tegemist on info omadusega, mille säilitamist peetakse hädavajalikuks, kuid mis ei ole piisav kinnitamaks, et mittepöörduva transformatsiooni käigus on sisuinfo säilinud adekvaatsel kujul. See on oluline omadus info autentsuse määratlemisel. Selline infotunnus sõltub esitusinfost, sealhulgas ka semantilisest infost (*semantic information*), mis näitab seda, kuidas info on kodeeritud ja mida see tähendab. Digiobjektide autentsuse kohta esitab info objekti looja või teabe üleandja digihoidlasse või -arhiivi üleandmise käigus. See teave moodustab osa säilituskirjeldusinfost (PDI). Arhiiv hoiab, uuendab ja vastavalt vajadusele täiendab seda teavet. Info looja võib esitada või ka arhiiv ise luua infotunnuste kirjeldused nende infotunnuste kohta, mille säilitamine on oluline. Infotunnuste kirjeldused moodustavad osa päritoluinfost (*provenance information*), näiteks EPUB-vormingus digiraamat, mis lugeri ekraanil esitatakse tavapäraste raamatulehekülgedena koos tekstilõikude, pealkirjade, ääriste, leheküljenumbritega jms. Tekst koosneb tähtedest, numbritest ja kirjavahemärkidest, mis on organiseeritud sõnadeks ja lauseteks. Kui me loeme infotunnusteks sõnad, kirjavahemärgid ja lõike eraldavad märgid, siis selle digiraamatu faili migreerimisel võivad muud vorminguosad minna kaduma, aga e-raamat loetakse endiselt autentseks. Infotunnuse kirjeldused oleksid sellisel juhul "lõigu määratlejad" ning "sõnu ja kirjavahemärke väljendavad märgid".

Säilitamisstrateegiate mõju digiobjektide autentsusele

Digitaalse kultuuripärandi autentsuse tagamine eeldab lisaks objekti ja selle konteksti tundmisele ka läbimõeldud, pikaajalisele kestlikkusele suunatud säilitamise strateegiaid. Erinevalt mittedigitaalsetest objektidest ei seisne digiobjekti säilitamine üksnes selle olemasolu tagamises, vaid hõlmab aktiivset ja korduvat sekkumist, mis seisneb näiteks vormingu uuendamises, andmekandjate vahetuses, kontrollis jms. Iga selline sekkumine võib mõjutada objekti autentsust, olgu siis biti tasandil või tähenduse ja käitumise tasandil.[41]

[41] Margaret Hedstrom, "Digital Preservation: A Time Bomb for Digital Libraries", *Computers and the Humanities* 31:3 (1997), 189–202.

Kõige otsesem viis digiobjekti tervikluse tagamiseks on bititasandi säilitamine ehk failide hoidmine muutmata kujul koos nende kontrollsumma salvestamise ja perioodilise ülevaatusega. Kontrollsumma, näiteks SHA-256 algoritmil põhinev väärtus, võimaldab tuvastada, kas faili bittides on aja jooksul toimunud soovimatuid muutusi. Selline faili muutumatuse kontroll on kõigi digiarhiivide elementaarne usaldusväärsuse tagamise mehhanism. Sellise lähenemise puhul eeldatakse, et kui kontrollsumma kehtib, on objekt terviklik ja seega ka autentne oma struktuurilisel tasandil. Siiski ei saa sellest järeldada, et objekt on ka semantiliselt või funktsionaalselt autentne. Eriti kultuuripärandi objektide puhul võib juhtuda, et säilitatakse küll identne fail, kuid selle kasutamise kontekst, seotud kirjeldused või funktsionaalsus on kadunud.[42]

Seetõttu peab bititasandi säilitamine olema seotud metaandmete halduse ja säilitusahela jälgimisega. Enamikes professionaalsetes säilitussüsteemides (nt DSpace, Rosetta, Archivematica) on muutumatuse kontroll integreeritud auditilogidesse, kuid selle tõhusus sõltub säilituskeskkonna järjepidevusest ja dokumenteerimisest. Bitijadade muutumatuna hoidmine ei ole üldjuhul sobiv strateegia digiobjektide pikaajaliseks säilitamiseks, kuna probleem on digiobjekti sõltuvuses konkreetsest riist- ja tarkvarast.

Migreerimine (*migration*) on kõige laialdasemalt kasutatav meetod, et pidada sammu pidevalt muutuva tehnoloogiaga. See tähendab digiobjektide ülekandmist ühest riist- või tarkvara keskkonnast teise, kusjuures vajaduse korral digiobjekte ka muudetakse. Migratsiooni kasuks räägib asjaolu, et tehnoloogilised platvormid vananevad ja failivormingud võivad muutuda loetamatuks, kui neid ei uuendata.[43] Migratsioon on aga autentsuse seisukohalt küllaltki problemaatiline sekkumine, kuna sellega kaasneb alati võimalus, et objekti olulised omadused muutuvad või kaovad. Seda eriti siis, kui tegemist on keerukate või mitmekihiliste objektidega (nt vektorgraafika, multimeedia, hüperlinkidega tekstid).

Oluline on, et iga migratsioon oleks tagasiulatuvalt auditeeritav. Üheks praktikaks on eelnevalt määratleda objekti olulised omadused ning kasutada migreerimisjärgseid kontrollimeetmeid, et hinnata, kas need omadused on säilinud. Muuseumides ja raamatukogudes, kus objektide visuaalne ja tähenduslik terviklikkus on sageli määrav, peab migratsiooniga kaasnema

---

42 Clifford Lynch, "Authenticity and Integrity in the Digital Environment: An Exploratory Analysis of the Central Role of Trust", *Authenticity in a Digital Environment* (Washington, D.C.: Council on Library and Information Resources, 2000), 32–50 (41). http://www.clir.org/pubs/reports/pub92/lynch.html.

43 Digital Preservation Coalition, „Preservation action", *Digital Preservation Handbook, 2nd Edition* (Digital Preservation Coalition, 2015). https://www.dpconline.org/handbook.

ka kasutajapoolne valideerimine, näiteks kuraator või spetsialist kinnitab, et objekt on säilinud tähendust omaval kujul.

Migreerimise kõrval on emuleerimine (*emulation*) teine suur meetodite rühm, mida kasutatakse digiobjektide säilitamisel. Emuleerimine tähendab ühe andmetöötlussüsteemi jäljendamist teisega nii, et see võtab vastu samu andmeid ja annab töötlemise järel samu tulemusi. Emuleerimisel säilitatakse digiobjekt selle algsel kujul, nagu see on loodud.[44] See tähendab, et tulevikus taasesitatakse objekt koos virtuaalse keskkonnaga (nt operatsioonisüsteem, tarkvaraversioon, brauser), milles see algselt töötas. Emuleerimise meetod peab tagama selle digiobjekti esitamiseks vajaliku tarkvarasüsteemi olemasolu siis, kui digiobjekti soovitakse kasutada.

Emulatsioon võimaldab säilitada objekte nende esialgsel käitumistasandil, mis on oluline näiteks interaktiivsete meediumite, multimeedia installatsioonide või veebilehtede puhul. Küll aga nõuab emulatsioon täpset keskkonna dokumenteerimist (sh süsteeminõuded, seosed), turvalist failide ja failisüsteemide säilitamist ning jõudluse ja kasutajaliidese usaldusväärset replikatsiooni. Autentsuse seisukohalt võimaldab emulatsioon säilitada objekti ehedust mitte ainult failitasandil, vaid ka selle tunnetuslikus ja interaktsioonilises mõttes. Seetõttu peetakse emulatsiooni eriti sobivaks kultuuripärandiga seotud keerukamate objektide puhul.[45]

Autentsuse tagamiseks on oluline ka digiobjekti versioonide säilitamine: iga kord, kui objekti muudetakse (nt vormingumuutuse või metaandmete lisamise käigus), tuleb säilitada eelmine versioon või vähemalt selle võrdlusväärtused. See võimaldab kontrollida, kas objekti esialgne tähendus või struktuur on säilinud ka hilisemates versioonides. Sarnane funktsioon on geograafiliselt hajutatud varundusel ja tõrkekindlal säilitusloogikal (nt LOCKSS – Lots of Copies Keep Stuff Safe), mis aitavad vältida andmekadu ja ühtlasi võimaldavad versioonidevahelist verifitseerimist.[46] Arhiivinduslikust vaatenurgast on see lähenemine kooskõlas autentsuse kui säilitusahela omadusega – iga muudatus peab olema jälgitav, põhjendatud ja taastatav.

Digitaalse autentsuse seisukohalt on määrav digiobjektide muutmiskaitse ja juurdepääsuhalduse strateegia. Kui objektidele on avatud ligipääs ilma piiranguteta, suureneb risk, et neid muudetakse tahtlikult või kogemata. Seetõttu rakendatakse arhiivides ja raamatukogudes ainukirjutusmälusid (Write-once-read-many, WORM), auditeeritavat logimist (kes,

---

44 Jeff Rothenberg, "Ensuring the Longevity of Digital Documents", *Scientific American*, 272:1 (1995), 42–47.

45 Dene Grigar, Stuart Moulthrop, *Traversals: The Use of Preservation Through Emulation in Born-Digital Literature* (Cambridge: MIT Press, 2017), 23–31.

46 LOCKSS Programme, Stanford University Libraries, https://www.lockss.org.

millal ja mida vaatas või muutis), digiallkirjastamist või digitaalseid pitsereid, pöördumatu arhiivimise protokolle (nt objekti lukustamine pärast säilitamist). Kombineerituna tugeva autentimise (nt sertifikaadid) ja säilitusahela dokumentatsiooniga võimaldavad need strateegiad hoida objekti puutumatuna nii bititasandil kui institutsionaalses mõttes.[47]

Kokkuvõttes tuleb digitaalse kultuuripärandi autentsuse säilitamisel kaaluda erinevaid strateegiad vahel, st teha kompromisse praktilisuse, autentsuse taseme ja ressursside olemasolu vahel. Iga säilitusstrateegia mõjutab ühel või teisel viisil objekti autentsust. Digiobjektide autentsuse säilitamine ei ole üksnes teoreetiline või tehniline probleem, vaid eelkõige institutsionaalne praktika, mis sõltub ressurssidest, pädevusest ja organisatsioonikultuurist.

Digiobjektide autentsuse tagamine Eesti mäluasutustes

Eestis tegeleb dokumendipärandi kogumise ja säilitamisega peamiselt Rahvusarhiiv, mille allüksusena tegutseva digitaalarhiivi põhiülesanne on digitaalarhivaalide kogumine, säilitamine, neile juurdepääsu võimaldamine ja kasutamise korraldamine.[48] Autentsuse tagamine on sealsete tööprotsesside keskmes, sest digitaalseid arhivaale saab kasutada teadusliku uurimistöö, juriidiliste tõendite või kultuurimälu alusmaterjalina ainult juhul, kui nende päritolu, terviklus ja käsitlemisahel on tõendatavad. Rahvusarhiivi käsitluses ei tähenda autentsus üksnes faili puutumata olekut, vaid kogu organisatsioonilise ja tehnilise raamistikuga loodud usaldusväärsust, mis hõlmab nii bititasandi terviklust, metaandmete ja konteksti fikseerimist kui ka säilitusprotsesside läbipaistvat dokumenteerimist.

Rahvusarhiivi digitaalarhiiv tugineb rahvusvahelistele standarditele. Alusmudeliks on OAIS (Open Archival Information System, ISO 14721), mis määratleb süsteemi põhikomponendid (vastuvõtt, hoid, juurdepääs) ning infopakettide loogika (SIP[49], AIP[50], DIP[51]). OAIS-i kõrval rakendatakse PREMIS-mudelit, mis määrab, milliseid säilitustegevuste metaandmeid

---

47 PREMIS Data Dictionary, Version 3.0 (Washington, D.C.: Library of Congress, 2015). https://www.loc.gov/standards/premis/v3/premis-3-0-datadictionary-only.pdf.

48 Rahvusarhiiv, *Digitaalarhiivi põhimäärus (2022)*. https://www.ra.ee/wp-content/uploads/2023/01/Digitaalarhiivi-pohimaarus.pdf.

49 Vastuvõtu infopakett – kontseptuaalne infohulk (mitte füüsiline kapseldatud fail), mis ühe üleandmise- vastuvõtu käigus üleandjalt digitaalarhiivi edastatakse (ingl Submission Information Package).

50 Säilituspakett, mis sisaldab digiinfo tagatisfaile (ingl Archival Information Package).

51 Kasutuspakett – juurdepääsu kontseptuaalne infopakett, sisaldab ainese kasutusfaile ja/või arhiivikirjeldust (ingl Dissemination Information Package).

tuleb talletada, et säilitusahel oleks auditeeritav. Lisaks järgitakse ISO 16363 põhimõtteid, mis kirjeldavad usaldusväärse digitaalarhiivi hindamiskriteeriume. Kohaliku infoturbe raamistikuna ei kasutata enam ISKE etalonturbesüsteemi, vaid seda asendab E-ITS (Eesti infoturbe standard), mis on hetkel rakendamisel. E-ITS-i audit on osaliselt käimas, kuid selle põhimõtteid saab juba praegu käsitada digiarhiivi autentsuse ja tervikluse tagamisel kohaldatavana.[52]

Autentsuse alus luuakse juba enne, kui digiobjektid jõuavad arhiivi. Rahvusarhiiv on rõhutanud, et kõige olulisem on nõuetele vastav dokumendihaldus arhiivimoodustaja juures. Kui asutus kasutab korrektset dokumendihaldustarkvara, mis tagab kasutajate autentimise, toimingute logimise ja dokumentide tervikluse, on võimalik üleandmisel säilitada ka usaldusväärne provenients. Digiallkiri ja ajatempel võivad seda täiendada, kuid ei asenda süsteemset dokumendihaldust.

Digiobjektide vastuvõtt toimub SIP-pakettidena, mis peavad sisaldama nii objekte kui ka metaandmeid vastavalt dokumenteeritud andmemudelile. Vastuvõtul genereeritakse igale failile kontrollsumma, mis salvestatakse metaandmetesse ja mida kasutatakse hiljem regulaarselt failide tervikluse kontrolliks. Provenientsi kirjeldus seob objekti loomiskonteksti ja loovutajaga, administratiivsed metaandmed dokumenteerivad õigused ja kasutustingimused, tehnilised metaandmed annavad ülevaate failivormingutest ning tegevuste metaandmed dokumenteerivad kõik arhiivi sees tehtud operatsioonid (nt migratsioon, teisendamine). Nimetatud toimingud tagavad, et säilitusahel on hiljem täielikult auditeeritav.

Rahvusarhiiv kasutab migreerimisstrateegiat, mille kohaselt hoitakse objekte pikaajaliselt sobivates säilitusvormingutes, näiteks PDF/A, TIFF, PNG, WAV või MPEG-4. Selleks on koostatud arhiivivormingute loetelu, mida ajakohastatakse regulaarselt, jälgides rahvusvahelist praktikat. Vajadusel viiakse läbi massmigratsioonid, mille käigus teisendatakse failid uutesse sobivatesse vormingutesse. Seejuures dokumenteeritakse kõik toimingud, et tagada failide sisu ja kasutatavuse säilimine ka tehnoloogia arenedes. Füüsilisel tasandil rakendatakse dubleerimist, arhivaalid säilitatakse vähemalt kahel koopial geograafiliselt eraldatud kohtades, hetkel *online* kettamassiivides ja magnetlintidel. Kandjate terviklust kontrollitakse, vigased koopiad asendatakse ja kõik toimingud logitakse. See välistab nii andmekao kui ka lugemistehnoloogia kadumisest tingitud riskid.

[52] "Eesti Infoturbestandard E-ITS", Riigi Infosüsteemi Amet, https://eits.ria.ee/ (22.11.2025).

Autentsuse tagamisel on oluline ka rollide ja vastutuste jaotus. Rahvusarhiivi süsteemis on selgelt määratletud rollid (vastuvõtuhaldur, hoiuhaldur, administraator, säilitamise planeerija jt), et välistada huvide konfliktid ja tagada nelja silma põhimõte kriitiliste toimingute puhul. Kõik tegevused logitakse muutmiskindlasse auditisüsteemi, kus on fikseeritud, kes mida tegi, millal ja millise töövahendiga.

Rahvusarhiivi digitaalse arhiveerimise analüüs rõhutas, et kuigi Rahvusarhiivi sisemine süsteem on rahvusvaheliselt eeskujulik, on suuremad probleemid arhiivimoodustajate juures: metaandmete puudulikkus, failide päritolu ebamäärasus ja killustatud dokumendihaldussüsteemid raskendavad autentsuse tõendamist. Analüüs soovitas vähendada dokumendihaldussüsteemide hulka ning ajakohastada arhiiviseadust ja arhiivieeskirja, et autentsuse mõiste ja tingimused oleks õigusraamistikus selgemalt määratletud.[53]

Kokkuvõttes moodustab Rahvusarhiivi autentsuse tagamise süsteem mitmekihilise terviku: bititasandi kontroll (kontrollsummad, koopiad), sisutasandi kontekst (provenients, metaandmed, üleandmise dokumentatsioon), protsesside läbipaistvus (tegevuste logid, auditeeritav migratsioon) ja institutsionaalne raamistik (OAIS, PREMIS, ISO 16363, ISKE).

Muuseumide infosüsteem MuIS on veebipõhine keskkond, mida kasutatakse muuseumikogude üle arvestuse pidamiseks ja nende haldamiseks. MuIS-i kaudu tehakse muuseumidesse koondatud teave kättesaadavaks nii erialaspetsialistidele kui ka kõigile teistele huvilistele. MuIS on Eesti muuseumide keskne andmekogu koos tööliidese ja avaliku veebiportaaliga, selle koosseisu kuulub ka digihoidla, kuhu võetakse pikaajalisele säilitamisele digitaalsed failid (digikujutised ja digitaalsed museaalid). Vastutav töötleja on Muinsuskaitseamet, teenuse tehniline osutaja Registrite ja Infosüsteemide Keskus (RIK). MuIS-i eesmärk on ühtlustatud arvelevõtt, toimingute elektrooniline registreerimine ning andmete avalikustamine. Digiobjektide autentsust toetavad nii haldus- kui tehnilised kontrollid (sh turbenõuded käideldavusele, terviklusele, konfidentsiaalsusele). MuIS-is on museaali kirjed seotud alusdokumentidega (nt omandamisotsused, väljaarvamise otsused, eksperthinnangud), mis aitab kinnitada päritolu ja toimingute juriidilise raamistiku ning hinnata autentsust.

MuIS-is kirjeldatakse objekte mitmel tasandil (sh olemus, materjal, tehnika, seisund, dateering). MuIS-i avalikus vaates näeb eeskätt sisu

[53] AS PricewaterhouseCoopers Advisors, Digitaalse arhiveerimise terviklik analüüs. Lõpparuanne (2016). https://www.ra.ee/wp-content/uploads/2016/12/digianalyys_pwc2016.pdf.

kirjeldavaid välju, kuid administratiivsed ja toimingutele viitavad väljad ei ole reeglina avalikud ja need jäävad sisekasutuse auditijäljeks. MuIS logib andmete esitamist ja päringuid ning kasutajaõiguste andmist ja äravõtmist. See loob kontrolljälje, mis on autentsuse hindamisel keskne (kes mida tegi, millal ja mis alusel). Andmete esitajad tuvastatakse kõrge turvalisusega vahenditega (ID-kaart, Mobiil-ID, Smart-ID). Juurdepääsupiirangud on määratletud: automaatselt piiratakse näiteks andmeandja isikuandmeid, teoste püsiasukohta ning ostuhinda, muud piirangud saab kehtestada muuseumi juht vastava taotluse alusel. Nii tekib kontrollitav vastutus (*accountability*), mis on autentsuse tagamise institutsionaalseks eelduseks.

MuIS digihoidla rakendab digitaalse säilitamise protsessis nii aktiivkui ka passiivsäilituse põhimõtteid.[54] Digitaalsete objektide vastuvõtul tuvastatakse ja täiendatakse metaandmeid ning luuakse kasutuspaketid, sealhulgas pisipildid. Ühe museaali kohta võib olla seotud mitu digitaalset objekti. Digiteerimisel luuakse eraldi säilituskoopia (tavaliselt TIFF-formaadis) ja kasutuskoopia (nt JPEG-formaadis). MuIS-i arhiveerimisfunktsioon on suunatud eelkõige säilituskoopia pikaajalisele talletamisele ning selle tervikluse ja autentsuse säilitamisele.

Avalikule kasutajale esitatakse digitaalsed objektid vastavalt õiguslikele piirangutele: autoriõiguste, isikuandmete või muude kitsenduste korral on nähtav üksnes pisipilt, samas kui piiranguteta objektid muutuvad avalikult kättesaadavaks pärast museaali arvelevõtu kinnitamist. Selline lahendus eristab selgelt avalikku esitamist, mille eesmärk on kasutatavus ja usaldus, ning säilituskoopiat, mis toimib digitaalse objekti autentsuse tõendusmaterjalina.

Kokkuvõttes toetub MuIS-i autentsuse tagamise süsteem institutsionaalsele vastutusele (MKA/RIK rollid ja turvapoliitikad), protsessikontrollile (standarditud vastuvõtutee ja metaandmed), tehnilistele lahendustele (digihoidla aktiiv-/passiivkiht, AIP/DIP, tagatisfailid) ning läbipaistvale auditijäljele (logid, alusdokumendid, tugev autentimine). See kombinatsioon annab usutava tõenduse, et avalikus vaates nähtav fail on see, mis ta väidab end olevat – ja selle taustal on olemas kontrollitav, kordus- ja ülevaatlik säilitusahel.

Eesti MAR-sektori digipöörde areng on olnud kiire, kuid ebaühtlane. Asutused seisavad silmitsi sarnaste katsumustega: objekti autentsuse

[54] Käesolevas artiklis kasutatakse mõisteid aktiiv- ja passiivsäilitus funktsionaalsete kihtidena digitaalse säilitamise protsessis, eristamaks kasutatavusele ja kontekstualiseerimisele suunatud tegevusi bititasemel säilitamisest ja autentsuse tagamisest.

tõendamine pikaajalisel säilitamisel, metaandmete järjepidevus, süsteemide migratsioon ja kasutajapõhine tähendusloome.

Digitaalse kultuuripärandi autentsuse hindamise raskused

Digiobjektide autentsuse säilitamine on kultuuripärandiga seotud digiarhiivides näiliselt tehniline küsimus, kuid praktikas on see sageli väärtuspõhine, kontekstitundlik ja epistemoloogiliselt keerukaks tegevus. Kui arhiivinduse klassikaline autentsuse mõiste lähtub objekti identiteedist ja terviklusest kui tõenduspädevuse eeltingimustest, siis kultuuripärandi valdkonnas tuleb arvestada lisaks objekti mitmetähenduslikkuse, loovuse, institutsionaalse tõlgenduse ning kasutajate ootustega.

Kultuuripärandi digiarhiivide objektid ei ole pelgalt dokumendid klassikalises arhiivinduslikus mõttes, vaid need võivad olla ka interpretatsioonilised, protsessipõhised või interaktsioonil põhinevad. Selliste objektide puhul ei ole alati võimalik, ega ka mõttekas täpselt määrata, milline nende konkreetne olek on autentne. Selliste objektide näidetena võib tuua virtuaalnäituse, mille digiobjekte muudetakse igal eksponeerimisel või konserveerimisprotsessi dokumentatsiooni, mis muutub koos projekti edenemisega. Helisalvestiste korral kasutatakse sagedasti uusversiooni loomist või heli puhastamist, mis muudab küll heli puhtamaks, kuid samas eemaldab ajaloolise tekstuuri. Kõige selle tulemusena võib autentsus osutuda nö liikuvaks sihtmärgiks. Küsimus ei ole ainult "kas see objekt on ehtne", vaid ka "millise tähenduseversiooni suhtes see on ehtne". Selline olukord seab kahtluse alla traditsioonilise käsitluse, mille kohaselt autentsus on objekti staatiline omadus.

Teine probleemidering ilmneb seoses tehnilise ja kultuurilise autentsusega. Digiarhiivides kasutatavad tehnilised säilitusmehhanismid, nagu kontrollsummad, digiallkirjad ja standardiseeritud failivormingud, võimaldavad tuvastada, kas digitaalne objekt on bititasandil muutmata. Need mehhanismid tagavad arhivaari seisukohast objekti tehnilise autentsuse, kuid ei ole enamasti kasutajale vahetult mõistetavad ega tõlgendatavad. Seetõttu ei lähtu kasutaja digitaalse objekti hindamisel tehnilistest kontrollmehhanismidest, vaid teeb oma järeldused muude, talle arusaadavamate tunnuste alusel, nagu visuaalne esitlus, kirjeldav kontekst ja seosed teiste objektidega. Sellises olukorras võib tehniliselt autentne, kuid kontekstualiseerimata digitaalne fail tunduda kasutajale moonutatud, ebapiisav või isegi "tähenduseta". Samuti võib originaalist tuletatud derivaat tunduda veenvam või autentsem tänu paremale esitusele või sellega kaasnevale narratiivsele taustale. Kasutaja vaates ei pruugi olla oluline, kas fail

on identne originaaliga, vaid see, kas fail on esitletud arusaadavalt, läbipaistvalt ja kontekstitundlikult. Seega võib autentsus tähendada kasutajale ka usutavat lavastust või rekonstruktsiooni (nt interaktiivne simulatsioon). Sellises käsitluses on autentsus performatiivne kvaliteet – midagi, mis toimub läbi taasesituse. See ei välista arhiivinduslikku autentsust, kuid nõuab selle täiendamist.

Autentsus on tihedalt seotud usaldusega (*trust*). Kasutajate usaldus on sageli seotud institutsiooni mainega, mitte niivõrd konkreetse tehnilise protsessiga.[55] See viitab autentsusele kui usaldussuhtele, kus tehniline tõend ei pruugi kattuda sotsiaalse või kultuurilise veendumusega. Autentsus pole ainult objekti omadus, vaid suhe objekti, säilitaja ja kasutaja vahel. Klassikalised autentsuse määratlused rõhutavad, et objektid peavad olema tõepoolest need, milleks neid väidetakse. Sellest tuleneb aga küsimus, kes ja millises protsessis kinnitab või tunnustab digitaalse objekti autentsust ning millisel hetkel see otsus kehtestatakse.

Autentsuse hindamisel ja tagamisel on oluline ka institutsionaalne võimekus. MAR-sektori analüüsid on näidanud, et digihalduse ja kontrollmehhanismide kasutus on asutuste lõikes ebaühtlane – suurematel asutustel on tavaliselt välja arendatud kontrollsummade ja säilitusahela töövood, kuid väiksemates muuseumides ja raamatukogudes võivad need olla osaliselt rakendatud, ebaregulaarsed või katta üksnes osa säilitusahelast. See ei tähenda, et võimekus puudub kogu sektoris, vaid praktika on heterogeenne ja sõltub ressursist, tehnilistest vahenditest ja koolitusest. Autentsuse haldamine nõuab standardiseeritud, kuid paindlikke töövooge ja asjakohast koolitust nii konservaatoritele, kuraatoritele kui ka infosüsteemide haldajatele.

Kokkuvõte

Digiajastul tekib üha rohkem digitaalsel kujul loodud kultuuripärandit, mida tuleb säilitada. Sellise pärandi autentsuse tagamine on keerukas, kuna objekti identiteet, terviklus ja tähendus on kergesti muudetavad

[55] Clifford Lynch, "Authenticity and Integrity in the Digital Environment: An Exploratory Analysis of the Central Role of Trust", *Authenticity in a Digital Environment* (Washington, D.C.: Council on Library and Information Resources, 2000), 32–50 (41). http://www.clir.org/pubs/reports/pub92/lynch.html; RLG/OCLC Working Group on Digital Archive Attributes, *Trusted digital repositories: attributes and responsibilities* (Mountain View, CA: Research Libraries Group, 2002); RLG-NARA task force on digital repository certification, *Trustworthy repositories audit & certification: criteria and checklist* (Chicago: Center for Research Libraries, 2007), www.crl.edu/PDF/trac.pdf; http://www.crl.edu/sites/default/files/d6/attachments/pages/trac_0.pdf.

ning klassikalised arhiivinduslikud käsitlused vajavad olulist täiendamist. Digikeskkonnas ei tulene autentsus mitte objekti puutumatust füüsilisest kandjast, vaid institutsionaalsetest praktikast, säilitusahelast ja metaandmetest. See muudab autentsuse küsimuse vähem staatiliseks omaduseks ja rohkem protsessiks, mis eeldab läbipaistvat juhtimist. Digitaalse autentsuse küsimus kultuuripärandiga seotud digiarhiivides on ühtaegu nii tehniline, institutsionaalne kui kultuuriline. Artiklis näitasin, et traditsiooniliselt arhiivindusest pärinev autentsuse kontseptsioon, mis keskendub objekti identiteedile ja terviklusele on digitaalkeskkonnas saanud juurde uusi aspekte, mis ulatuvad failistruktuurist kuni kasutajaootuste ja semiootilise tõlgendusteni. Seetõttu on vajadus käsitleda autentsust mitte ühtse kvaliteedina, vaid mitmetasandilise ja kontekstitundliku süsteemina, kus fail, kontekst, kasutus ja institutsiooniline raamistik moodustavad ühtse, kuid mitte lõpliku tõendusahela.

Kultuuripärandi digiarhiivides ei tähenda autentsus üksnes bititasandi või failistruktuuri säilimist, vaid ka kultuurilise tähenduse ja konteksti säilimist. Kuraatorid, kogukonnad ja kasutajad loovad autentsust läbi kasutuse, esitluse ja tõlgenduse. Selline lähenemine nihutab autentsuse kontseptsiooni lähemale usaldusväärsusele ja epistemoloogilisele läbipaistvusele: oluline pole ainult see, kas objekt on tehniliselt muutumatu, vaid ka see, kas teda saab usaldada kui teadlikult hallatud ja tähenduslikult kestvat artefakti.

See uudne autentsuse käsitlus ei piirdu üksnes digiobjektidega. Samad põhimõtted, läbipaistev dokumenteerimine, kontekstitundlik haldus ja tähenduslik säilitamine, on rakendatavad ka mittedigitaalsete kultuuripärandi objektide autentsuse puhul. Olgu tegemist arhiividokumendi, museaali või kunstiteosega, autentsuse tagamine eeldab üha enam teadlikku ja reflektiivset lähenemist, mis arvestab lisaks objekti füüsilisele seisundile ka selle tähenduslikku rolli kultuurilises ja institutsionaalses raamistikus. Seega võib digiobjektide autentsuse ümbermõtestamine avada uusi võimalusi kogu kultuuripärandi läbipaistvamaks ja kasutajakesksemaks säilitamiseks.

Märksõnad: digitaalse kultuuripärandi autentsus; digiarhiivindus; digiobjektid; institutsionaalne usaldus; digiobjekti olulised omadused

Kurmo Konsa on Tartu Ülikooli ajaloo ja arheoloogia instituudi arhiivinduse kaasprofessor ja Kõrgema Kunstikooli Pallas professor. E-post: kurmo.konsa@ut.ee.

Abstract: *Ensuring the authenticity of digital cultural heritage*

This article examines the concept of authenticity in the preservation of digital cultural heritage, arguing that authenticity in digital environments cannot be reduced to technical fixity or bit-level integrity alone. Drawing on archival theory, international standards, and developments in digital preservation, the study traces the historical evolution of authenticity from provenance- and object-based criteria toward institutional, procedural, and context-dependent models. Particular attention is paid to the layered nature of digital objects—physical, logical, and conceptual—and to the role of metadata, preservation workflows, and documented chains of custody in sustaining authenticity over time.

The article further demonstrates that authenticity in digital cultural heritage operates simultaneously on technical, institutional, and cultural levels. While archival systems rely on formal mechanisms such as checksums, controlled workflows, and standardised metadata, users often assess authenticity through contextual clarity, narrative coherence, and institutional trust rather than through technical evidence. This divergence highlights authenticity as a relational and performative quality, shaped by interactions between objects, custodial institutions, and users.

Using the Estonian memory institutions sector as a contextual frame, including archival and museum information systems, the article shows how authenticity is actively produced and maintained through institutional responsibility, standardised yet flexible preservation practices, and transparent documentation. The study concludes that digital authenticity should be understood as a dynamic, multi-layered process rather than a fixed attribute, requiring continuous management, contextualisation, and critical reflection. This reconceptualisation has implications not only for digital heritage, but also for broader historical and museological approaches to authenticity.

Keywords: digital heritage authenticity; digital archiving; digital objects; institutional trust; significant properties

Kurmo Konsa is Associate Professor at the Institute of History and Archaeology (Tartu University) and Professor at the Pallas University of Applied Sciences. E-mail: kurmo.konsa@ut.ee.