1. Perusteet

1.1. Valtion tietohallinto ja tietohallintopolitiikka

1.1.1. Tietotekniikan käyttö ja kehityssuunta

Valtionhallinnon tietotekniikkatoiminnan menot olivat valtiovarainministeriön suorittaman selvityksen mukaan vuonna 1990 yhteensä 2.250 miljoonaa markkaa. Vuotta aikaisemmin menot olivat 1.897 miljoonaa markkaa. Valtionhallinnon atk-menot kasvoivat 1980-luvulla keskimäärin noin 20 prosenttia vuodessa.

Tietojenkäsittelyn volyymin nopea nousu ja tästä aiheutuva atk-riippuvuuden kasvu edellyttävät valtion virastojen, laitosten ja liikelaitosten turvallisuustoimenpiteiden huomattavaa tehostamista yhtenäisen tietoturvallisuuspolitiikan avulla.

Edellä mainitun selvityksen mukaan hallinnon käytössä oli vuoden 1991 syyskuun alussa suuria, keskisuuria ja pientietokoneita yhteensä 2.134, mikrotietokoneita 52.011 ja päätelaitteita 20.366 kappaletta. Suurten, keskisuurten ja pientietokoneiden määrä oli kolminkertaistunut viidessä vuodessa. Samassa ajassa mikrotietokoneiden määrä oli kolmetoistakertaistunut.

Laitteistoluvut merkitsevät samalla sitä, että lähes joka kolmas, useissa virastoissa jo joka toinen palveluksessa oleva (henkilöstön kokonaismäärä noin 208.000) käyttää työssään omaa tai yhteiskäytössä olevaa työasemaa. Valtionhallinnon palveluksessa olevista henkilöistä runsaat 3.900 toimii päätoimisesti tietotekniikkatehtävissä. Valtionhallinto on täten laitteiden määrän ja päätoimisen henkilöstön perusteella laskettuna suurin tietotekniikan käyttäjä Suomessa.[1]

Vertailun vuoksi voidaan todeta Kunnallishallinnon atk-neuvottelukunnan (KATKO) suorittaman selvityksen perusteella, että vuonna 1991 kunnallishallinnon atk-menojen kokonaismäärä oli noin 1.348 miljoonaa markkaa.[2] Koska kyselyyn ei saatu aivan kaikilta yksiköiltä vastausta, niin KATKO on arvioinut kokonaismenojen olleen kaikkiaan noin 1,5 miljardia markkaa.

---

[1] Ks. tarkemmin "Tietoja valtionhallinnon tietotekniikkatoiminnasta 1991", Valtiovarainministeriö, Helsinki, 1992.

[2] Ks. "Tietoja kunnallishallinnon tietotekniikasta 1991", Kunnallishallinnon atk-neuvottelukunta, Helsinki 1991.

Tietokoneita eli suuria, keskisuuria ja pientietokoneita oli vastanneilla yhteensä 884. Mikrotietokoneita kunnallishallinnossa ja kuntien oppilaitoksissa oli yhteensä noin 40.000. Näyttöpäätteiden määrä oli 24.650. Kunnallishallinnon palveluksessa olevan päätoimisen tietotekniikkahenkilöstön määrä oli noin tuhat.

Tämä vertailu osoittaa, että päätoimisten atk-henkilöiden sekä laitteistojen määrä valtionhallinnossa on edelleen selvästi suurempi kuin kunnallishallinnossa ja suhteutettuna palveluksessa olevaan henkilöstöön valtionhallinnon automaattisen tietojenkäsittelyn hyödyntämisaste on myös huomattavasti suurempi. Toisaalta valtionhallinnon hoitamat tehtävät poikkeavat kunnallishallinnon tehtävistä ja täten mainittujen lukujen suora vertailu antaa aina hieman virheellisen kuvan kokonaistilanteesta.

Valtionhallinnossa tietotekniikkaa käytetään kaikilla hallinnonaloilla ja tasoilla. Suurimpia käyttäjiä ovat suurista toiminnallisista perusrekistereistä ja järjestelmistä vastaavat virastot,[3] tutkimus- ja kehitystoiminta, opetustoiminta ja normaalit hallinnollisia tehtäviä hoitavat virastot. Yleisimmin käytettyjä sovelluksia ovat toimistojärjestelmät, joiden perusrungon muodostavat tekstinkäsittely- ja laskentaohjelmistot sekä talous- ja henkilöstöhallintoon liittyvät sovellukset.

Tuskin mikään tekninen kehitys on johtanut niin syvällekäyviin rakenteellisiin muutoksiin kaikilla elämänaloilla kuin nykyaikainen informaatioteknologia. Tähän vaikuttaa osaltaan myös tietoliikenteen infrastruktuurin kehittyminen digitalisoinnin myötä erilliset tietojärjestelmät kiinteästi yhdistäväksi verkoksi.

Vuonna 1991 telelaitosten rekistereissä oli yli 120.000 datasiirtomodeemia. Datasiirto kasvaa noin 20 % vuodessa, kun perinteisessä puhelinliikenteessä kasvu on noin 4 %. Nämä luvut pätevät useimmissa teollisuusmaissa ja osoittavat osaltaan yhteiskunnan tietokoneistumista.

Yhteenvetona voidaan sanoa, että koko julkisen hallinnon toiminta ja palvelukyky sekä koko maan kansainvälinen kilpailukyky on suurelta osin tiedollisen ja samalla tietoteknisen osaamisemme varassa.

[3] Kuten mm. väestörekisterikeskus, valtiokonttori, tilastokeskus, verohallitus ja maanmitttaushallitus.

1.1.2. Tietohallintopolitiikka ja tietoturvallisuus

Valtionhallinnon tietohallinnon ohjaus on osa yleistä valtioneuvoston suorittamaa hallinnon ohjausta. Valtioneuvoston tietotekniikan käytölle ja tietohallinnolle asettamien tavoitteiden saavuttaminen edellyttää yhteisiä periaatteita ja yhteensovittavia toimenpiteitä.

Tietoturvallisuus on puolestaan osa tietohallinnon ohjausta ja tietotekniikan käytön kehittämistä. Sitä ei ole syytä nähdä erillisenä asiana, mutta sen kehittäminen edellyttää myös omia linjauksia ja ohjeitaan, kuten tässä muistiossa tullaan esittämään.

Tietoturvallisuus on huomioitu valtionhallinnon tietohallintoasetuksen (155/88) 1 §:ssä, jonka mukaan virastojen ja laitosten tietojenkäsittelyä ja tietohallintoa on kehitettävä siten, että tietojärjestelmät edistävät valtionhallinnon tavoitteiden saavuttamista ja ovat taloudellisia, turvattuja, toiminnallisesti yhteensopivia sekä tietosuojan vaatimukset täyttäviä. Valtioneuvoston päätös valtion tietohallinnon kehittämisestä edellyttää myös turvallisuusnäkökohtien huomioon ottoa kaikissa olosuhteissa.[4]

Näiden peruslinjausten lisäksi valtiovarainministeriö on antanut 1970-luvulta alkaen valtionhallinnolle erillisiä hallinnollisia ohjeita tietoturvallisuuden yleisestä kehittämisestä ja eräistä sen osa-alueista. Lisäksi muiden ministeriöiden ja eräiden virastojen toimesta on annettu hallinonala- ja virastokohtaisia täydentäviä tietoturvallisuusohjeita.

1.2. Tiedon merkityksen kasvu ja uhkakuvan muuttuminen

Tiedon merkitys on kasvanut automaattisen tietojenkäsittelyn ja tietoliikenteen kehityksen myötä. Länsimaiset yhteiskunnat ovat kokeneet toisen teollisen vallankumouksen, informatiikan vallankumouksen, ja siirtyneet tietoyhteiskunnan aikakauteen. Automaattinen tietojenkäsittely on muuttanut tiedon merkitystä siten, että siitä on tullut lähes korvaamaton voimavara niin hallinnossa ja liike-elämässä kuin yhteiskunnassa yleensäkin.

Tietoturvallisuuspolitiikan laatiminen on tullut välttämättömäksi nimenomaan sen vuoksi, että nykyiseen yhä kasvavassa määrin tietojenkäsittelyn varaan rakentuvaan valtionhallintoon ja koko yhteiskuntaan kohdistuu entistä enemmän tiedon käyttöön, säilymiseen ja teknisten laitteiden toimivuuteen liittyviä uhkateki-

[4] Valtiovarainministeriö 22.3.1989, no J 182/750/89.

jöitä. Nämä riskit on tarpeen tunnistaa ja luoda riskienhallintatyölle kestävä pohja. Parhaiten se käy päinsä johdonmukaisen tietoturvallisuuspolitiikan avulla.

Tietoteknisestä riippuvuudesta aiheutuvat uhkatekijät voivat vaarantaa ja häiritä jokapäiväisiä toimintojamme niin normaaliaikana kuin poikkeusoloissakin. Tietojen määrän kasvu ja niiden voimakas keskittyminen atk:lle on muodostanut uuden, aikaisempaa riskialttiimman tilanteen. Suuretkin tietokannat voivat tuhoutua joko inhimillisen toiminnan, tekniikan puutteiden, onnettomuuksien ja vahinkojen tai luonnontapahtumien vuoksi, ellei niiden suojaamiseksi ole ryhdytty asianmukaisiin turvallisuustoimenpiteisiin.

Tietoturvallisuuden avulla voidaan varmistaa niin valtion, erilaisten yhteisöjen kuin yksityisten kansalaisten perusintressejä. Tietoturvallisuuden puute vaarantaa ja voi aiheuttaa vahinkoa mm. organisaation toiminnalle, taloudelle, valtion turvallisuudelle ja kansainvälisille suhteille, finanssi-, raha- ja valuuttapolitiikan hoidolle, valvonta- ja tarkastustoimelle sekä rikosten ehkäisemiselle.

Vieraiden valtioiden samoin kuin yritystenkin harjoittama tiedustelutoiminta kohdistuu nykyään entistä enemmän teknisten, kaupallisten, hallinnollisten ja taloudellisten yrityssalaisuuksien anastamiseen. Yritysvakoilun keinoin voidaan nopeasti ja verraten vähäisin kustannuksin päästä laittomasti hyödyntämään huomattavia henkilö- ja pääomaresursseja vaatineita tutkimus- ja kehittelytyön tuloksia. Kilpailukykymme säilyttämisen vuoksi tietoturvallisuustoimenpiteitä on syytä tältäkin osin tehostaa sekä julkisella että yksityisellä sektorilla.

Yksityisten kansalaisten taloudelliset edut, pankkisalaisuus, lääkintäsalaisuus ja muut laisäädäntömme mukaan salassa pidettävät intressit samoin kuin yksilöiden suojelu henkilötietojen automaattisessa tietojenkäsittelyssä ovat myös riippuvaisia tietoturvallisuuden tasosta.

Maksuliikenteen automatisointi valtionhallinnossa samoin kuin yleensä liike-elämässä on johtanut siihen, ettei suuri osa rahavaroista ole enää perinteiseen tapaan fyysisessä muodossa seteleinä, vaan tietokoneiden muisteissa. Rahat samoin kuin yrityssalaisuudet on ennenkin voitu anastaa, mutta nykyään se voi käydä päinsä myös sähköisesti, tietoverkkojen avulla ja vaikkapa maapallon toiselta puolen. Tämäntyyppisten tietotekniikkarikosten suorittaminen voi käydä perinteisiin tekotapoihin verraten nopeasti ja monesti lähes jälkiä jättämättä, ellei tietoturvallisuudesta ole kunnolla huolehdittu.

1.3. Tietoturvallisuuden kansainvälinen kehittämistyö

Euroopan Neuvoston *(CoE, Council of Europe)* tietoturvallisuuspoliittinen päätös hyväksyttiin maaliskuun 31 päivänä 1992. Kansainvälisen taloudellisen yhteistyön ja kehityksen järjestön, OECD:n *(Organization for Economic Co-operation and Development)* vastaava päätös on odotettavissa syksyllä 1992. Tätä kirjoitettaessa käytettävissä olevat CoE:n[5] ja OECD:n[6] asiakirjat edellyttävät jäsenvaltioiden määrittelevän ensi tilassa oman tietoturvallisuuspolitiikkansa.

Ruotsin hallitus teki tietoturvallisuuspoliittisen linjanvetonsa neljä vuotta sitten hallituksen julkistaessa lähes 50 sivuisen tietohallintopolitiikkansa, josta tietoturvallisuuspolitiikkaa koskeva osuus oli yhdeksän sivua. Amerikan Yhdysvalloissa vahvistettiin vuonna 1988 valtionhallinnon tietoturvallisuuslaki. Norja kaavailee omaa vielä luonnosasteella olevaa tietoturvallisuuslakiaan ja asetustaan saatettavaksi voimaan asteittain ylimenokautena 1993-1996.

Kysymyksessä ovat Yhdysvaltain ja Norjan osalta nimenomaan *tietoturvallisuuden erikoislait* eivätkä niitä normihierarkisesti alemmanasteiset *Policy*-linjaukset, joita on tällä hetkellä olemassa Ruotsin lisäksi mm. Saksassa ja Kanadassa.[7]

Liitteenä 3 on ei-julkinen *vertaileva katsaus* tietoturvallisuuden kehittämisestä eräiden kansainvälisten organisaatioden yhteistyönä sekä selvitys Ruotsin, Norjan, Saksan, Amerikan Yhdysvaltojen ja Kanadan tietoturvallisuuspoliittisista perusratkaisuista.

Tietoturvallisuuden merkityksen yleisestä kasvusta on edelleen selvänä osoituksena Yhdistyneiden Kansakuntien laaja-alainen ja voimaperäinen tietoturvallisuuden kehitystyö. YK on keskittynyt tie-

---

[5] *COUNCIL DECISION in the field of Security of Information Systems* , Proposal submitted by the Commission on 27 July 1990, Council Decision of 31 March 1992, 92/242/EEC, Official Journal of the European Communities 8.5.92 No L 123/19.

[6] OECD asetti vuonna 1989 asiantuntijatyöryhmän laatimaan tieturvallisuuspolitiikan suuntaviivoja. Näiden *Guidelines for the Security of Information Systems* ydin on ilmaistu seuraavasti: "In implementing the principles the *governments are urged* among other things *to adopt appropriate and coherent computer security policies.*" - Hallituksilta siis edellytetään asianmukaista ja yhdensuuntaista tietoturvallisuuspolitiikkaa. Kyseisen asiantuntijajärjestön päätöksillä on jäsenvaltioihin nähden kuitenkin ainoastaan moraalista, ei sensijaan EY:n direktiivien tavoin kansainoikeudellisesti sitovaa merkitystä.

[7] Eri asia on, että lähes kaikissa OECD ja EY maissa on jo olemassa yksityisyyden suojaa, tekijänoikeutta ja tietotekniikkarikoksia koskevaa muuta tietoturvallisuuteen liittyvää lainsäädäntöä.

totekniikkarikosten torjuntaan sekä alajärjestöjensä kautta erityisesti tietoliikenteen (*International Telecommunications Union*, ITU) turvaamiseen.

Kansainvälinen standardisoimisjärjestö *International Organization for Standardization*, ISO,[8] kansainvälinen rikospoliisijärjestö *I.C.P.O. - Interpol*, kansainvälinen tulliyhteistyöjärjestö *Customs Co-operation Council*, CCC, ja lukuiset elinkeinoelämän puitteissa toimivat organisaatiot kuten kansainvälinen kauppakamarijärjestö *International Chamber of Commerce*, ICC, tekevät myös tällä hetkellä laaja-alaista ja voimaperäistä tietoturvallisuuden kehitystyötään.[9] Myös Suomi on ollut aktiivisesti mukana useissa näistä toiminnoista.

Kansainvälinen tietoliikenne ja tietojärjestelmät vaativat turvatoimien asianmukaista huomioon ottamista kaikilta osapuolilta. Tämä johtuu pohjimmaltaan siitä, että tietoturvallisuus on ns. heikoimman lenkin ilmiö. Kansainväliset yhteisöt ja niiden jäsenet eivät voi omien etujensa vuoksi sallia turvallisuustyhjiöiden muodostumista. Heikot lenkit vaarantavat kokonaisuudet ja niiden osat mitätöiden samalla ne voimavarat, joita asianmukaisen turvallisuuden luomiseksi on muualla uhrattu.

Suomen vastaisuudessa yhä enemmän tietoon ja osaamiseen perustuvalle yhteiskunta- ja elinkeinoelämälle on tärkeätä, että ulkomaiset yhteyskumppanimme voivat pätevin perustein luottaa haluumme ja kykyymme huolehtia tietoturvallisuutemme tasosta. Suomen tietoturvallisuuspolitiikassa kirjatut periaatteet on nähtävä tuota *luottamusta lisäävänä* toimena.[10]

---

8 Yhteistyössä kansainvälisen sähkötekniikkakomission *International Electrotechnical Commissionin, IEC:n* ja kansainvälisen puhelin- ja lennätinliikenteen neuvottelukomitean *Comité Consultatif International de Telephonique et Telegraphiquen, CCITT:n* kanssa. ISO:n ja muiden järjestöjen tietoturvallisuustyötä käsitellään tarkemmin tämän taustamuistion ei-julkisessa liitessä 3.

9 Customs Co-operation Council on julkaissut teoksen *"An Introduction to EDI in Customs"*, jonka 13 luku on omistettu tietoturvallisuudelle. International Chamber of Commerce on julkaissut *"Uniform Rules of Conduct for the Exchange of Commercial Data via Telecommunications Networks"*.

Huomattava kuitenkin on, että organisaatioiden välisen tiedonsiirron oikeudellinen perusta on edelleen luonnosasteella. Standardissa ISO 9735 (EDIFACT) on määritelty säännöstö OVT-sanomien muodostamisesta, mutta asianmukaiset turvallisuusjärjestelyt ovat edelleen työn alla.

10 Vastaava argumentti sisältyy Hallituksen esitykseen Eduskunnalle rikoslain kokonaisuudistuksen toisen vaiheen käsittäväksi rikoslain ja eräiden muiden lakien muutoksiksi, (s. 372, moniste, Oikeusministeriö, huhtikuu 1992).

1.4. Tietoturvallisuuden peruskäsitteet ja osa-alueet

Tietoturvallisuudella *(Information Security)* tarkoitetaan tietojen, järjestelmien ja palveluiden asianmukaista suojaamista sekä normaali- että poikkeusoloissa lainsäädännön ja muiden toimenpiteiden avulla. Tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä suojataan laitteisto- ja ohjelmistovikojen, luonnontapahtumien tai tahallisten, tuottamuksellisten ja tapaturmaisten inhimillisten tekojen aiheuttamilta uhilta ja vahingoilta.

Tietoturvallisuus rakentuu periaatteessa *tiedon (Information)* kolmen eri ominaisuuden - luottamuksellisuuden, eheyden ja käytettävyyden - varaan.

Luottamuksellisuudella tarkoitetaan sitä, että tiedot ovat vain niihin oikeutettujen henkilöiden tai yhteisöjen saatavissa eikä niitä paljasteta tai muutoin saateta sivullisten käyttöön.

Eheydellä tarkoitetaan sitä, etteivät tietoaineistot ja järjestelmät ole laitteisto- ja ohjelmistovikojen, luonnontapahtumien tai oikeudettoman inhimillisen toiminnan seurauksena muuttuneet tai tuhoutuneet.

Käytettävyydellä tarkoitetaan sitä, että järjestelmien tiedot ja niiden muodostamat palvelut ovat tarvittaessa niihin oikeutettujen henkilöiden tai yhteisöjen esteettä hyödynnettävissä.

Tietoturvallisuus voidaan suunnittelun, toteutuksen ja valvonnan kannalta jakaa kahdeksaan osa-alueeseen:

1) *Hallinnollinen,*
2) *Henkilöstö-,*
3) *Fyysinen-,*
4) *Tietoliikenne-,*
5) *Laitteisto-,*
6) *Ohjelmisto-,*
7) *Tietoaineisto- ja*
8) *Käyttöturvallisuus.*

1.5. Tietoturvallisuuspolitiikan soveltamisala

Valtionhallinnon tietohallintoasetuksen ja tietohallinnon kehittämistä koskevan valtioneuvoston tietohallintopäätöksen kohteena ovat ministeriöt, virastot ja laitokset. Vastaavalla tavalla muistiossa esitetyn tietoturvallisuuspäätöksen kohteena tulisivat olemaan vain valtionhallintoon kuuluvat organisaatiot eli *ministeriöt, virastot ja laitokset.*

Laitoksilla tarkoitetaan tässä yhteydessä myös *valtion liikelaitoksia*, koska monet niistä hoitavat valtion kannalta hyvin keskeisiä tehtäviä. Tämän vuoksi on tarpeen varmistaa, että myös niiden tietoturvallisuus täyttää muille valtionhallinnon yksiköille asetetut vaatimukset.[11]

Tietoturvallisuuspolitiikka koskee siis ensisijaisesti organisaatioita. Käytännössä se ei kuitenkaan voi toteutua toivotulla tavalla, elleivät myös yksittäiset *atk-käyttäjät* tunne politiikan sisältöä ja sitoudu toimimaan sen mukaisesti. Täten tietoturvallisuuspolitiikan kohteena tulee olla myös kaikki valtionhallinnon palveluksessa olevat tietotekniikan käyttäjät.

Valtionhallinnon lisäksi tietoturvallisuutta käsittelevän päätöksen periaatteita tulisi mahdollisuuksien mukaan noudattaa myös valtionhallinnon organisaatioiden sekä muiden organisaatioiden (kunnallishallinnon yksiköt, yritysmaailma) välisessä tietoteknisessä yhteistyössä ja tiedonsiirrossa. Tietoturvallisuuspäätöksen laajemmalle vapaaehtoiselle hyväksikäytölle työryhmä ei näe esteitä.

Mitä nimenomaan tulee valtionhallinnon tietohallintotoimintojen ns. ulkoistamiseen *(Outsourcing)*, niin tietoturvallisuusvastuun on katsottava säilyvän palvelua tilaavalla virastolla ja laitoksella itsellään. Vastaava periaate on ilmaistu henkilörekisterilain 3 §:ssä, jossa kirjattu yleinen huolellisuusvelvoite koskee sekä rekisterinpitäjää että tämän toimeksiannosta toimivia.

Toimeksianto ei siis vapauta viraston ja laitoksen johtoa tietoturvallisuusvelvoitteensa toteutuksesta eikä sitä voi pätevästi siirtää toimeksisaajalle. Eri asia on, että myös toimeksisaaja vastaa osaltaan viraston ja laitoksen tietojen turvallisuudesta. Tämä *tietoturvallisuusvastuun siirtämättömyyden* periaate tulisi myös aina kirjata näkyviin asianomaisiin toimeksiantosopimuksiin.

---

[11] Esimerkkeinä voidaan tässä mainita muiden muassa. Valtion tietokonekeskus, Posti- ja telelaitos, Valtionrautatiet ja Valtion painatuskeskus.

2. Tietoturvallisuuden käsite, osa-alueet ja riskien hallinta

2.1. Tietoturvallisuuden käsite

2.1.1. Yleistä

Edellä kohdassa 1.4. esitetty tietoturvallisuuden määritelmä kaipaa luonnollisesti sisältönsä tarkempaa erittelyä. Seuraavassa hahmotetaan määritelmän eri komponentteja: luottamuksellisuutta, eheyttä ja käytettävyyttä, tietoturvallisuutta tavoitetilana, suojan kohteita, hyvää tietoturvallisuustapaa ja suojaustason asianmukaisuuden yksilöintiä sekä tietoturvallisuuden suhdetta yksityisyyden suojaan.

Itse perustermiä *tietoturvallisuus* on pidettävä sanavalintana parempana ja johdonmukaisempana (vrt. liikenneturvallisuus, säteilyturvallisuus, yleinen järjestys ja turvallisuus) kuin lyhennettä "tietoturva".[12] Terminologisen selkeyden saavuttamiseksi ns. "tietosuojasta" käytetään tässä yhdenmukaisesti julkisuuslakiehdotuksen kanssa ilmausta *yksityisyyden suoja (Privacy Protection).*[13]

2.1.2. Luottamuksellisuus, eheys ja käytettävyys

Tästä tietoturvallisuuskäsitteen ytimen muodostavasta kolminaisuudesta käytetään kansainvälisissä tietoturvallisuuspäätöksissä ja alan ammattikirjallisuudessa vakiintuneesti englanninkielisiä termejä *Confidentiality, Integrity, Availability.*[14]

Tietoturvallisuuteen kohdistuvat uhat ja vahingot, tietojen asiaton paljastuminen *(luottamuksellisuuden menetys)*, tietojen muuttuminen tai muuttaminen *(alkuperäisen sisällön eheyden menetys)* ja vaikutukset tietojen oikea-aikaiseen saatavuuteen sekä järjestelmien ja palvelujen toimivuuteen halutulla tavalla ja haluttuun

---

[12] Esimerkiksi 1.8.1991 voimaantulleessa L:ssa arvo-osuusjärjestelmästä käytetään termejä *tieto- ja rekisteriturvallisuus* (15 §:n 1 momentin 4 kohta).

[13] Julkisuuslain 24 §:n otsikko on *Yksityisyyden suoja.* Henkilörekisterilainsäädännössä on käytetty vanhahtavaa termiä "tietosuoja" tarkoitettaessa yksityisyyden suojaa.

[14] Ruotsinkielisissä lähteissä vastaavat käsitteet ovat *Förtrolighet, Integritet* ja *Tillgänglighet.* Saksan tietoturvallisuusviraston perustamista koskevan lain alussa määritellään termit *Vertrautlichkeit, Unversehrtheit* ja *Verfügbarkeit.* Ranskalaisissa normeissa käytetään ilmauksia *La Confidentialite, L'Integrite* ja *La Disponibilite.*

aikaan *(käytettävyyden menetys)*, on myös mahdollista kuvata riittävän täsmällisesti näiden ominaisuuksien puitteissa.

Eheyteen laajassa mielessä voidaan katsoa kuuluvan myös tietoaineiston todistusarvoon liittyvät *oikeaperäisyyden* ja *koskemattomuuden* ominaisuudet.[15] Tiedon eheyteen voidaan myös sisällyttää tietoliikenteen todistusoikeudelliseen arvoon liittyvä *kiistämättömyys*. Viimemainittu *Non-Repudiation*-ominaisuus vastaa esimerkiksi perinteistä kirjatun kirjeen saantitodistusta tai haasteen tiedoksiantotodistusta.

Oikeaperäisyydellä, koskemattomuudella ja kiistämättömyydellä tulee olemaan ratkaiseva merkitys, kun kansainväliseen kauppaan osallistuvat maat pyrkivät huolehtimaan tietojärjestelmiensä turvallisuudesta niin, että ne täyttävät kaikkiin sovellettavat yhteiset standardit.

Luottamuksellisuuden, eheyden ja käytettävyyden muodostaman kokonaisuuden turvallisuusvaatimukset samoin kuin niiden tärkeyden keskinäiset painotukset vaihtelevat tapauksittain. Henkilörekisterilain vaatiman yksityisyyden suojan toteuttaminen käytännössä edellyttää luottamuksellisuusnäkökohtien asianmukaista huomioon ottamista. Luottamuksellisuus on erityisen tärkeätä useissa ulkoasianhallintoon ja maanpuolustukseen liittyvissä järjestelmissä. Valtion maksuliikenteen turvallisuus ja julkinen luotettavuus vaativat myös korkeata suojaustasoa tietojen eheyden suhteen. Käytettävyyden merkitys puolestaan korostuu erityisesti hälytys- ja ajantasaisissa varausjärjestelmissä.

---

15 Ruotsissa on valmistumassa asiasta perusteellinen selvitys rikoslain väärennystä koskevan uudistuksen yhteydessä. Tällä selvityksellä on erityisesti merkitystä EDI:iin liittyvässä uudessa oikeudellisessa arvioinnissa pyrittäessä lain säännöksillä turvaamaan kattavasti tämä uusi kaupankäynnin muoto. Oleellista tietojen vaihdon eheyden ja oikeustoimen sitovuuden kannalta on, että lähettäjä ja kaupan kohteen sisältö ovat oikeita ja että sopimuksen syntyminen voidaan riidan syntyessä pätevästi todistaa.

Oikeaperäisyys ja koskemattomuus ovat todistettavissa teknisen turvallisuusmenetelmän (numerolukko eli salakirjoitus), kiistämättömyys puolestaan todistettavissa olevan kuittauksen tai luotettavan kolmannen osapuolen tiedoston avulla. Näihin ominaisuuksiin nojautuu myös Ruotsin tullilain (1990:138) 12 a §:n nykyaikainen *elektronisen asiakirjan* määritelmä: "Med ett elektronisk dokument avses en upptagning vars innehåll och utställare kan verifieras genom ett visst tekniskt förfarande." Kysymys on siis tallenteesta, jonka sisällön koskemattomuus *(Bonitas)* ja laatijan oikeaperäisyys *(Veritas)* voidaan perinteisen oikeudellisen (kriminalistisen) asiakirjatutkimuksen keinojen sijasta todentaa teknisen tietoturvallisuusmenetelmän avulla.

2.1.3. *Tietoturvallisuus tavoitetilana*

Koska täydellinen tietoturvallisuus samoin kuin turvallisuus yleensä on käytännössä mahdoton saavuttaa, niin kysymyksessä on asianmukaisen suojaamisen *tavoitetila*, joka saadaan aikaan riittävien turvallisuustoimenpiteiden avulla.

Vaikka asianmukaisen tietoturvallisuuden tavoitetila sinänsä toteutetaankin järjestelmällisin toimenpitein, niin itse turvallisuus ei käsitteenä kuitenkaan ole sen enempää yksittäinen toimenpide kuin toimenpiteiden kokonaisuuskaan. Turvallisuus on näiden toimenpiteiden tulos ja siis tila, johon niillä pyritään. Esimerkiksi ilmaliikenneturvallisuus tai tieliikenneturvallisuus ovat kumpikin kiistattomia tavoitetiloja. Niidenkin tiettyjen kriteerien mukainen taso ja standardit ovat toteutettavissa vain asianmukaisten ja riittävien liikenneturvallisuustoimenpiteiden avulla.[16]

Tässä omaksuttu tietoturvallisuuden tavoitetilan ajallinen ulottuvuus kattaa *sekä normaali- että poikkeusolot*. Rauhanajan toimenpiteet luovat perustan, jolle valmiussuunnittelu ja poikkeusolojen riskienhallinta rakentuu. Periaatteena on, että poikkeusoloissa noudatetaan pääosin samoja menetelmiä kuin normaalitilanteissa.

2.1.4. *Suojan kohteet*

Suojan kohteena ovat *tiedot* (esim. palkkatiedot), *järjestelmät* (esim. maksuliikennejärjestelmät) ja niiden muodostamat *palvelut* (esim. palkanmaksu). Tietoturvallisuutta ei kuitenkaan ole tarkoituksenmukaista rajata niin, että esimerkiksi perinteiset paperilla olevat tiedot jäisivät tietoturvallisuuskäsitteen ulkopuolelle. Päinvastoin, *asiakirjaturvallisuus* on, kuten jäljempänä havaitaan, eräs tietoturvallisuuden oleellisia ainesosia.[17] Järjestelmät voidaan ymmärtää teknisinä, palvelut puolestaan toiminnallisina kokonaisuuksina.

---

16 Saksan tietoturvallisuusvirastoa koskevan lain käsitemääritelmien mukaan tietoturvallisuus merkitsee tiettyjen *turvallisuusstandardien mukaisen tason toteuttamista* turvallisuustoimenpitein, jotka koskevat tietojen käytettävyyttä, eheyttä tai luottamuksellisuutta tietoteknisissä järjestelmissä (*BSI-Errichtungsgesetz*, 17.12.1990, 2 §).

17 Samaa tarkoittaen voidaan puhua sekä asiakirjaturvallisuudesta että tallenneturvallisuudesta. Asiakirjat ovat lyhyesti määriteltyinä oikeuselämässä relevantteja selityksiä. Tekninen tallenne on vain eräs asiakirjan fyysinen muoto. Tässä on kuitenkin omaksuttu yleisempi sanonta *tietoaineistoturvallisuus* lähinnä siksi, että asiakirja mielletään ennen kaikkea paperimuotoiseksi dokumentiksi. Tietoaineistoturvallisuus käsittää myös ihmisaivoissa olevien tietojen turvallisuuden hyväksi tehtävät toimenpiteet. (Ks. myös jäljempänä s. 24 s.).

Tietoturvallisuus koskee oleellisimmalta sisällöltään *tietoja* olivatpa ne materiaalisesti missä muodossa tahansa: paperilla, mikrofilmillä, sähköisessä, sähkömagneettisessa tai optisessa muistissa, tietoliikennekaapelissa tai ihmisaivojen muistipaikoissa. Suojeltaessa tietoja suojellaan samalla sekä laitteistoja että ohjelmia.

Datalla ja informaatiolla ei ole tässä suhteessa eroa. Informaatio on lyhyesti määriteltynä dataa, jolla on tietty lisäarvo ja relevanssi, kun taas data on sellaista raakatietoa, jota voidaan tietoteknisesti käsitellä. *Informaatioteoreettisesti* tässä on siis omaksuttu näkemys, jonka mukaan informaatio on aineellisen ja energeettisen ohella materian kolmas aspekti, joka ei voi esiintyä itsenäisesti aineesta ja tajunnasta riippumatta.[18]

Tietotekniikalla sinänsä tarkoitetaan tiedon automaattisen käsittelyn sekä siirron välineitä ja menetelmiä että niiden käytön osaamista.[19]

2.1.5. Hyvä tietoturvallisuustapa ja suojaustason asianmukaisuus

Hyvä tietoturvallisuustapa perustuu näkemykselle, että turvallisuustoimenpiteet on mitoitettava heijastamaan tietojen, järjestelmien ja palvelujen luottamuksellisuus-, eheys- ja käytettävyysvaatimuksia. Vaadittavan huolellisuuden määrä mitataan objektiivisesti. Sen tulee vastata sitä, mitä järkevät ja vastuuntuntoiset henkilöt pitävät tarpeellisena sellaisessa tilanteessa, mistä kulloinkin on kysymys.

Suojaustason *asianmukaisuus* ratkaistaan aina *in casu* eli kussakin yksityistapauksessa erikseen. Se riippuu kullakin elämänalalla ja tietojenkäsittelympäristössä vastaavissa tapauksissa noudatettavasta hyvästä tietoturvallisuustavasta.

Huolellisuusvelvoitteen mittapuu on siis samanlainen kuin esimerkiksi vahingonkorvausoikeudessa yleensä. Tietoturvallisuuden suhteen on noudatettava huolellisen henkilön noudattamaa standardia. Alan kansainvälisessä englanninkielisessä ammattikirjallisuudessa käytetään termejä *"Due Care"* ja *"Best Practice"* tarkoittamaan tätä

---

18 Ks. Otavan Suuri Ensyklopedia 3, hakusana *Informaatioteoria*. (s. 2067 ss.).

19 Tietotekniikan käsite oli määritelty tällä tavoin valtionhallinnon tietohallinnosta annetun asetuksen soveltamisohjeessa, Valtiovarainministeriö 1.3.1988, Nro 147/750/88, s. 1 (ei enää voimassa). Vastaava määritelmä sisältyy myös Tietotekniikan liiton Atk-sanakirjan viidenteen korjattuun painokseen (1990, s. 123).

tietoturvallisuuden juridisen sisällön ydintä. Esimerkiksi pankkien kansainvälisessä ja kansallisessa maksuliikenteessä samoin kuin henkilörekisterien pidossa on jo olemassa tällainen huolellisuusvelvoitteen vertailuperusta. Monilla muilla aloilla turvallisuutta koskevat mittapuut ovat kuitenkin vasta muotoutumassa.

Henkilörekisteriä pitävältä edellytetään kaikessa rekisterinpitoon liittyvässä toiminnassaan erityistä huolellisuutta ja valppautta yksityisyyden suojaan liittyvien riskien tunnistamisessa ja erilaisten haittojen ennaltaehkäisyssä. Henkilökisterilain 3 §:ään onkin kirjattu yleinen huolellisuusvelvoite, joka koskee sekä rekisterinpitäjiä että hänen toimeksiannostaan toimivia ja henkilötietoja rekisterinpitäjiltä saaneita. Rekisteritoiminnassa on noudatettava hyvää rekisteritapaa.

Vaikka hyvän rekisteritavan sisältöä ei vielä voidakaan täysin tyhjentävästi osoittaa, niin sen sisältö täsmentyy jatkuvasti soveltamiskäytännön myötä. Samankaltaisia oikeudellisia ilmiöitä ovat eräät muutkin joustavat oikeuskäsitteet kuten hyvä kirjanpitotapa, hyvä kauppiastapa ja hyvä merimiestapa. Myös ne muotoutuvat ajan mukana vastaamaan kulloisiakin tarpeita. Useasti toistettuina ne katsotaan velvollisuudeksi.

2.1.6. Tietoturvallisuus ja yksityisyyden suoja

Yksityisyyden suoja liittyy oleellisesti tietoturvallisuuden luottamuksellisuuskomponenttiin. Henkilörekisterien luottamuksellisuus samoin kuin niiden eheys ja käytettävyyskin ovat *tietoturvallisuutta*, intiimien tietojen käyttörajoitukset ja niiden kontrolli sen sijaan puhtaasti yksityisyyden suojaa *(Privacy Protection)*. Käyttörajoitusten kontrollia ei toteuteta tietoturvallisuustoimenpitein, vaan erityisesti sitä varten perustetun, kansalaisten yksityisyyden suojaa valvovan virkakoneiston toimesta.

Rekisterinpitäjän huolellisuusvelvoite henkilötietoja kerättäessä, talletettaessa, käytettäessä ja luovutettaessa koskee yksityisyyden suojan ohella myös *valtion turvallisuutta*. Viimemainittu on selvästi tietoturvallisuuteen eikä yksityisyyden suojaan liittyvä yleinen intressi. Sitä ei ole edes mahdollista aikaansaada ja ylläpitää intiimien tietojen käyttörajoitusten viranomaisvalvonnalla, vaan ainoastaan asianmukaisin tietoturvallisuustoimenpitein.

Tietoturvallisuuden rinnalla käytetty termi "tietosuoja" on nähtävissä jossain määrin vanhahtavana ja harhaanjohtava. Suomen kielen sana tieto kattaa niin "datan" kuin "informaationkin", mikä ti-

lanne itse asiassa tarkemmin selvitettynä vallitsee myös muissakin kielissä.[20] Selvyyden vuoksi on siis perusteltua puhua tietoturvallisuudesta yläkäsitteenä ja "tietosuojan" sijaan *yksityisyyden* suojasta, kun tarkoitetaan tiettyjä yksilön intiimien tietojen käytön rajoituksia ja käyttörajoitusten kontrollitoimenpiteitä.

Tietoturvallisuus ei ole pelkästään teknisin keinoin tapahtuvaa suojausta, vaan sen oleellisia ainesosia ovat hallinnollinen-, henkilöstö- ja käyttöturvallisuus. Nimenomaan *hallinnollinen turvallisuus* laajassa mielessä sisältää normatiivisen komponentin, joka ulottuu erittäin monelle oikeusalalle.

Esimerkkejä ovat suunnitteilla olevat tietotekniikkarikokset huomioon ottavat rikoksentekijäin luovuttamista ja tutkintasäännöksiä koskevat kansainväliset sopimukset, kansainvälisten järjestöjen tietoturvallisuuspäätökset, turvallisuusstandardit ja tietoliikennenormit sekä kansallisella tasolla tietoturvallisuuslait, rikoslait, rikosprosessilait tai tietoturvallisuuspoliittiset periaatelinjaukset.

Havainnollinen ja läheinen esimerkki on tämän muistion esitys valtionhallinnon tietoturvallisuuspäätökseksi. Se samoin kuin kaikki vuosien varrella annetut alemmanasteiset ohjeet ja suositukset ovat vallan muuta kuin pelkin teknisin keinoin tapahtuvaa suojausta.

Asianlaita käy ilmi edellä esitetyn lisäksi alan kansainvälisten järjestöjen puitteissa vakiintuneesta tietoturvallisuuden määritelmästä sekä jäljempänä tarkemmin yksilöityjen tietoturvallisuuden oleellisien ainesosien kuvauksesta.

---

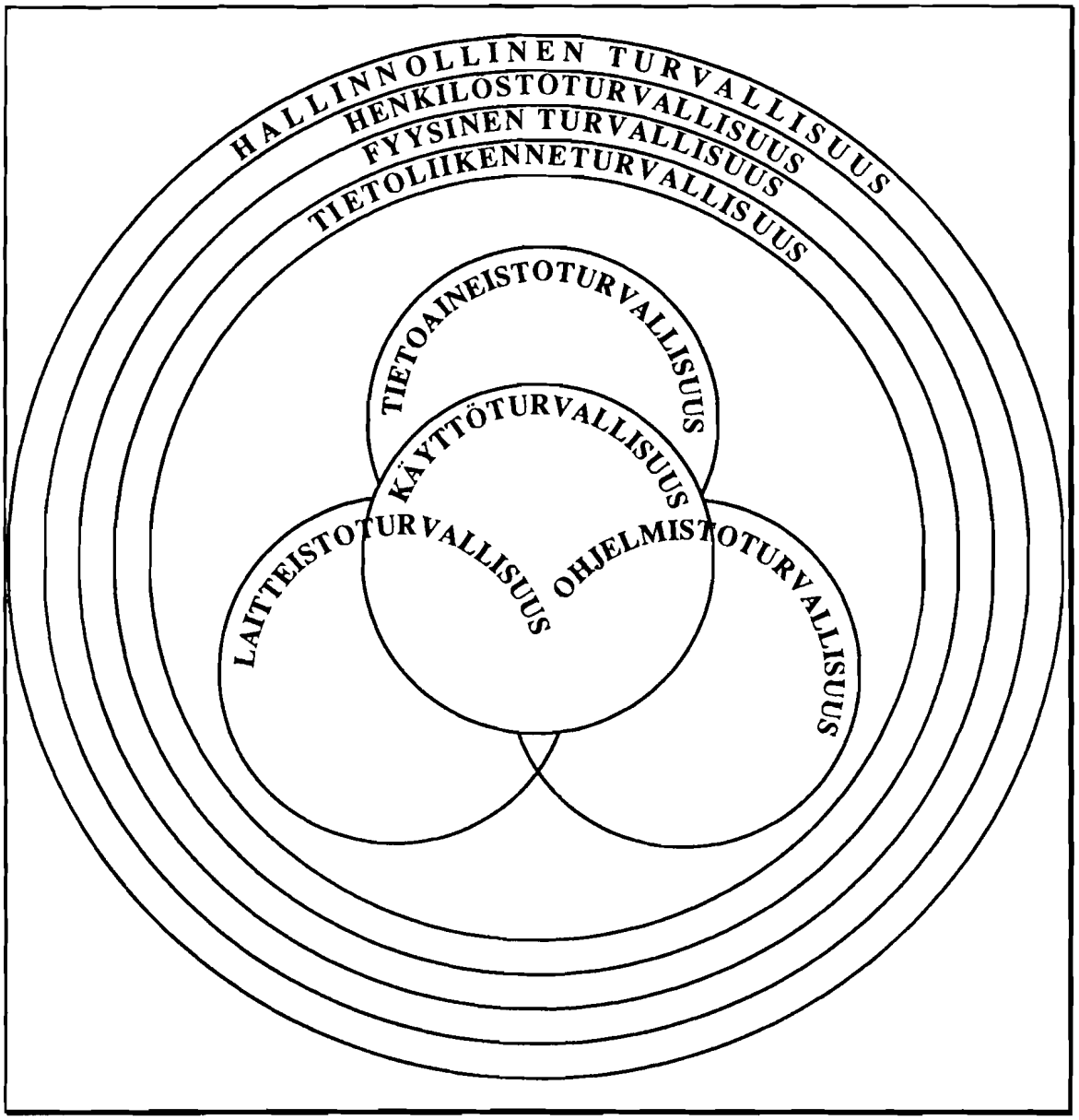
[20] Tiedon alkeisyksikkö *bitti* (Bit, Binary DigiT) sisältää jo informaation "Kyllä/Ei". Tilanteesta riippuen sillä voi olla jo sellaisenaan suuri merkitys (esim. maihinnousukäsky tai sen peruutus). *Data Security* ja *Information Security* ovat siten samaa tarkoittavia käsitteitä.

Etenkin 1970-luvulla käytetyn "Data Protectionin" sijasta on uudemmassa kansainvälisessä tietoturvallisuutta käsittelevässä kirjallisuudessa alettu yksityisyyden suojasta käyttää termiä *"Privacy Protection"*. Samoin uudemmat yksityisyydensuojalait (esim. Kanadan) ovat englanninkielellä *Privacy* Acteja. Terminologia on siis kehittynyt ja selkiytynyt vasta ajan mukana.

2.2. Tietoturvallisuuden osa-alueiden määrittely

2.2.1. Yleistä

Kaikki alla olevassa kuvassa 1 esitetyt ainesosat niihin kuuluvine ja jäljempänä tarkemmin yksilöityine alakohtineen muodostavat kokonaisuuden, jossa *heikoin rengas määrää sen kestävyyden.* Turvallisuustoimenpiteiden laatu ja laajuus luonnollisesti vaihtelevat ympäristöjen mukaan, mutta niin yksittäisten mikrojen kuin laajojen tietoverkkojenkin suojaukseen liittyvät osa-alueet ja perusperiaatteet ovat kuitenkin pääosin samoja.



KUVA 1, *Tietoturvallisuuden oleelliset ainesosat, Essentials of EDP Security, The Eight Layer Protective Ring.* Lähde: TBS&RCMP, 1990.

Huomattavaa on, että turvallisuustoimenpiteet voivat ja usein osittain kuuluvatkin samanaikaisesti useampaan eri pääryhmään. Esimerkiksi tietojen turvallisuusluokitus niiden luottamuksellisuuden perusteella kuuluu sekä ryhmään hallinnollinen turvallisuus että ryhmään tietoaineistoturvallisuus. Samoin tietoturvallisuuskoulutus kuuluu sekä hallinnolliseen että henkilöstöturvallisuuteen.

Kysymyksessä on kokonaisuuden hallinta. Tietoturvallisuuden osa-alueiden muodostaessa useita vyöhykkeitä vasta niiden muodostama kokonaisuus tarjoaa riittävän joustavuuden ja lujuuden uhkia ja oikeudenloukkauksia vastaan. Mikäli hallinnollisen-, henkilöstö- ja fyysisen turvallisuuden useinkin halvat ja yksinkertaiset perustoimenpiteet laiminlyödään ja niiden sijaan korostetaan liiaksi kalliita, teknisesti monimutkaisia laitteistoon ja ohjelmistoon liittyviä erikoisominaisuuksia, on kokonaisturvallisuuden kannalta päädytty väärään ja epätaloudelliseen ratkaisuun. Strateginen lähtökohta on hallinnollinen turvallisuus. Sen kattamaan alaan kuuluvat, kuten edellisellä sivulla oleva kuvio *(The Eight Layer Protective Ring)* havainnollisesti osoittaa, kaikki muutkin tietoturvallisuuden osa-alueet.

Näiden tietoturvallisuuteen liittyvien yleiskäsitteiden tuntemus auttaa viraston ja laitoksen johtoa hahmottamaan käytännössä tietoturvallisuuden kokonaisuuden, sen suhteet ja olennaiset piirteet laadittaessa virastokohtaisia suunnitelmia. Peruskäsitteiden ja -rakenteen ollessa kaikilla yhtenäiset helpottuvat turvallisuussysteemien toteutus ja tarkastettavuus samalla merkittävästi.

Edellä esitetyn kahdeksan toisiaan täydentävää turvallisuusvyöhykettä sisältävän ajatusmallin mukaisesti on myös mahdollista käsitellä ja arvioida seuraavan kaltaisia *turvallisten tietojärjestelmien* toteuttamiseen kuuluvia *perustoimintoja ja ominaisuuksia*:[21]

1) *Tunnistaminen ja todentaminen*, esimerkiksi tietojen ja ohjelmien pääsynvalvonnan käyttäjätunnukset ja salasanat, tunnistuksen varmentaminen erityistoimella,

2) *Käyttöoikeuksien hallinta*, esimerkiksi käyttöoikeustaulukot, joissa määritellään sellaiset toimenpiteet kuten luku, kirjoitus, suoritus ja lähettäminen,

[21] Sekä Amerikan Yhdysvalloissa että Euroopassa on erityisiä laitoksia tietojärjestelmien turvallisuuden arviointia ja luokitusta *(Information Technology Evaluation and Certification)* varten. Tässä mainitut kriteerit ja esimerkit on poimittu Saksan tietoturvallisuusviraston *(Bundesamt für Sicherheit in der Informationstechnik)* uusimmista julkaisuista.

3) *Käytön todentaminen lokitiedoston avulla* on erittäin tärkeä turvallisuusominaisuus, joka tulee ottaa suunnittelussa huomioon jo alunperin, sillä lokitiedostojen muuttaminen jälkiä jättämättä on useissa sovellusohjelmissa edelleen valitettavan helppoa,

4) *Muistialueen uudelleenkäyttö,* muistialueen tyhjääminen siten, ettei se sisällä suojattavaa jäännöstietoa,

5) *Järjestelmän toimintavarmuus,* esimerkiksi ohjelma- ja tiedonsiirtovirheiden käsittely käyttöjärjestelmän ja virheitä tunnistavan ja korjaavan protokollan puitteissa ja

6) *Tiedonsiirron turvallisuusominaisuudet,* esimerkiksi pääsynvalvonta, lähettäjän ja vastaanottajan sekä viestin sisällön todentaminen ja kiistämättömyys.[22]

2.2.2. *Hallinnollinen turvallisuus*

Hallinnollisella tietoturvallisuudella *(Administrative and Organizational Security)* tarkoitetaan niitä toimenpiteitä, joilla määrätään noudatettavista periaatteista ja toimintalinjoista yleensä. Hallinnolliseen turvallisuuteen kuuluu jo asian luonteesta johtuen organisatorinen turvallisuus, minkä vuoksi sitä ei ole käsitteen nimessä enää erikseen mainittu.

Tietoturvallisuus on pohjimmiltaan hallinnollinen ongelma, jonka ratkaisu turvallisuus-, toipumis- ja valmiussuunnitelmien avulla edellyttää mm. vastuiden ja organisaation määrittelyä, tietovarojen kartoitusta ja luokitusta, riskien arviointia ja hallintaa, ohjeistusta, neuvontaa ja koulutusta sekä valvontaa ja tarkastusta.

Hallinnollinen turvallisuus on kaikkien muiden osa-alueiden strateginen lähtökohta, joka kattaa myös teknisluonteisten suojauskeinojen tuntemisen ja hyväksikäytön.

---

22 Kaikkia edellä lueteltuja tietoliikenne-, laitteisto-, ohjelmisto-, tietoaineisto- ja käyttöturvallisuuteen kuuluvia seikkoja on osin varsin yksityiskohtaisestikin käsitelty valtiovarainministeriön atk-toiminnan loogista suojausta koskevassa ohjeessa (VM 14.1.1991 no 52/01/91) ja siihen liittyvässä vuodelta 1987 olevassa ei-julkisessa mietinnössä. Vielä täsmällisemmin niitä on kuitenkin eritelty esim. Saksan tietoturvallisuuskriteerien määrittelyteoksessa *Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik* luvussa 3 *(Grundfunktionen sicherer Systeme).*

*Tietoturvallisuus*suunnitelmilla tarkoitetaan perusturvallisuuden suunnittelua ja toteutusta sekä *toipumis*suunnitelmilla normaaliolojen katasrofitilanteiden varalle laadittavia järjestelmiä. Atk-*valmius*suunnitelmilla puolestaan ymmärretään Suomessa omaksutun terminologian mukaan poikkeusoloihin liittyvää turvallisuussuunnittelua.[23]

Turvallisuustoimenpiteiden mitoitusta varten valtiovarainministeriö on 1985 ja 1989 antanut ohjeet virastojen ja laitosten *atk-tärkeysluokituksesta*. Luokitusta on jonkin verran muutettu alkuperäisestä ja tällä hetkellä on meneillään uusi tarkistustyö. Luokitusta vahvistettaessa on otettu huomioon virastojen ja laitosten atk-toiminnan jatkuvuus- ja turvaamistarpeet erityisesti poikkeusoloissa.

Hallinnollisen tietoturvallisuuden osalta on syytä kiinnittää huomiota siihen, että turvallisuusjärjestelyjen tuleminen ulkopuolisten tietoon saattaa tehdä tällaiset järjestelyt kokonaan tarkoituksettomiksi. Tämän vuoksi julkisuustoimikunnan mietintöön (1992:9) sisältyvään julkisuuslakiesitykseen (25 §:n 5 kohta) kirjattu voimassaolevaa oikeutta selventävä periaate *turvallisuusjärjestelyjen salassapidosta* on tärkeä.

2.2.3. Henkilöstöturvallisuus

Henkilöstöturvallisuudella *(Personnel Security)* tarkoitetaan henkilöstöön liittyvien luotettavuusriskien hallintaa toimenkuvien, käyttöoikeuksien määrittelyjen sekä turvallisuuskoulutuksen ja valvonnan avulla. Henkilöstö on organisaation tärkein voimavara, mutta se saattaa olla myös suurin riskitekijä. Henkilöstöturvallisuustoimenpiteet ulottuvat vakinaisen ja tilapäisen henkilökunnan virka- ja työsuhteiden alkamis- ja päättymistilanteiden, tehtäväsiirtojen ja sijaisuusjärjestelyjen ohella myös vierailijoihin sekä ulkopuolisten palvelujen ostoon hanke-, huolto-, siivous- tms. sopimusten puitteissa.

Henkilöstöturvallisuuteen kuuluvat virka- tai työsopimussuhteessa virastoon tai laitokseen olevien omien työntekijöiden luotettavuuden valvontaan kuuluvat toimenpiteet. Se ulottuu myös ulkopuolisiin, sikäli kuin heillä on virastoon tai laitokseen tietty kiinnekohta, kuten esim. siivojilla tai kutsutuilla vierailijoilla. Mikäli virasto tai laitos turvautuu siivousliikkeen palveluihin on siivoojien taustan selvittäminen oleellinen henkilöstöturvallisuuskysymys.

---

[23]Ks. Tietojenkäsittelyn turvaaminen ja valmiussuunnittelu-opas, 1989, s. 9-10.

Vastaavat henkilöstöriskit liittyvät hanke- ja huoltosopimuksiin. Henkilöstöturvallisuustoimenpiteiden soveltamisala laajenee tietotekniikkaan liittyvien toimintojen ns. ulkoistamisen myötä. Henkilöstöturvallisuuden piiriin eivät sensijaan kuulu täysin ulkopuoliset henkilöt, kutsumattomat vieraat tai tietotekniset järjestelmiin murtautujat *(System-Hackers)*. Kysymyksessä on tuolloin lähinnä fyysiseen turvallisuuteen kuuluvat kulunvalvonta ja vartiointi sekä tietoliikenteeseen, laitteistoon, ohjelmistoon, tietoaineistoon ja käyttöön liittyvä turvallisuus. Eri asia on sitten, että ulkopuoliset voivat lahjoa tai pakottaa viraston tai laitoksen henkilökuntaa.

Selvyyden vuoksi on vielä mainittava, että henkilöstön taustojen tarkistukset esim. palvelukseen otettaessa ovat henkilöstöturvallisuutta, mutta tehtävien eriyttäminen (kuten sääntö, että kassanhoitajana ja kirjanpitäjänä on oltava eri henkilö) on käyttöturvallisuuteen kuuluva periaate samoin kuin tehtävien kahdentaminenkin (varamies- ja sijaisuusjärjestelyt käytön jatkuvuuden takaamiseksi). Käytön turvallisuuteen liittyvästä periaatteesta eikä tiettyjen henkilöiden luotettavuudesta on kysymys tallelokeroiden ja holvien avaimenhallintaan liittyvässä kahden avaimen järjestelmässä.

Tehtäväsiirroissa ja sijaisuusjärjestelyissä henkilöstöturvallisuus tulee kysymykseen sikäli, että on selvästikin syytä tarkistaa taustaa aiempaa perusteellisemmin siirrettäessä tietty palveluksessa jo oleva henkilö tehtävään, jossa vaaditaan erityistä luotettavuutta esimerkiksi valtion turvallisuuden vuoksi.

2.2.4. Fyysinen turvallisuus

Fyysisellä turvallisuudella *(Physical and Environmental Security)* tarkoitetaan laitteisto-, käyttö- ja varastointitilojen, arkistojen sekä laitteiden ja materiaalien fyysistä suojaamista. Fyysinen turvallisuus kattaa laajan alan aina ympäristö-, rakennus- ja rakennesuunnittelusta alkaen. Siihen kuuluvat myös kulunvalvonta, tekninen valvonta ja vartiointi sekä palo-, vesi-, sähkö-, ilmastointi- ja murto- ym. vahinkojen torjunta. Fyysiseen turvallisuuden piiriin voidaan katsoa kuuluvan myös tietoainesta sisältävien lähetysten ja kuriirien suojaamisen.

Ns. hajasäteilysuojaus (TEMPEST) ja suojaus elektromagneettista pulssia (EMP) vastaan on tässä luettu fyysiseen (rakenteelliseen) ja laitteistoturvallisuuteen. Ne on mahdollista lukea myös ainakin osit-

tain laitteistoturvallisuuteen ja tietoliikenneturvallisuuden yhteydessä erikseen käsiteltyyn ns. elektroniseen turvallisuuteen.[24]

Rajanveto fyysisen ja laitteistoturvallisuuden välillä voidaan suorittaa siten, että mikäli laitteet (kuten mikro tai lasertulostin) kiinnitetään alustaan (lattiaan pultattuun pöytään) anastusta estävin ratkaisuin (lattaraudoituksella tai vaijerilla) on kysymyksessä fyysinen turvallisuus. Sensijaan kovalevyn käynnistyslukko tai korttien ja muiden komponenttien anastuksen estävät tekniset ratkaisut ovat jo laitteistoturvallisuutta. Laitteistoturvallisuutta ovat myös omaisuudenmerkintätoimenpiteet, jossa esim. viraston tai laitoksen mikrot ja lasertulostimet merkitään poliisilta saatavin merkintävälinein (kynät ja kaivertimet).[25]

Palon- ja murronkestävät kaapit ovat fyysistä turvallisuutta, mutta asiakirjojen, levykkeiden, nauhojen, laitteistojen (kovalevyn, salkkumikron tai tiedostopalvelijan) sijoittaminen yöksi kassakaappiin ovat samalla tietoaineisto-, laitteisto- ja käyttöturvallisuutta.

Fyysisen turvallisuuden suhteen on oleellista kyetä sovittamaan yhteen perinteinen ja tietotekninen turvallisuusosaaminen erityisesti uusien järjestelmien ja tietojenkäsittelytilojen suunnittelu- ja rakennusvaiheessa. Valtiovarainministeriö on 12.12.1989 antanut rakennushallitukselle ohjeen turvallisuusnäkökohtien huomioon ottamiseksi valtion toimitiloissa.[26] Turvallisuusjärjestelyjen vaatima rahoitus hoidetaan samanaikaisesti tapahtuvan rakentamisen rahoituksen kanssa eli sisällytetään kohteen rakennusmäärärahoihin.

Ohjeessa käsitellään toimitilojen suunnittelun, rakentamisen ja käytön turvallisuusnäkökohtia. Pyrkimyksenä on yhdenmukaistaa turvallisuusjärjestelyjen toteuttamista ja auttaa oikean turvallisuustason määrittämisessä kussakin kohteessa. Ohje sisältää hallinnon-

---

[24] *Communications and Electronic Security.*

[25] Omaisuuden merkintä ja luettelonti ovat välttämätön edellytys varkauksien torjunnalle. Virastoilla ei yleensä ole kunnollista inventaaria hallinnassaan olevista mikroista ja päätelaitteista, joita vuonna 1991 oli tilastojen mukaan 72.377 kappaletta. Puhumattakaan siitä, että niiden sijainti olisi kuvattu piirroksena tai että ne olisi merkitty, kuten valtionhallinnossa nykyään Saksan Liittotasavallassa vaaditaan. Uusinta Suomessakin yksityisellä sektorilla sovellettua tekniikkaa edustaa mikrojen ja oheislaitteiden vaikeasti poistettavissa oleva "polttomerkintä" jo tehtaalla.

Mikrojen varkaudet ovat viime aikoina hälyttävästi lisääntyneet mm. Yhdysvalloissa, Saksassa ja Ruotsissa, joten vastatoimet ovat ajoissa paikallaan myös meillä. Keskusrikospoliisin ylläpitämän omaisuusrekisterin mukaan huhtikuussa 1992 oli anastettuja tietotekniikkaan liittyviä omaisuusesineitä Suomessa kateissa kaikkiaan 7.640 kappaletta.

[26] VM:n kirje rakennushallitukselle, No 4/04/84/12.12.1989.

aloittaisen luettelon turvallisuustasoluokituksesta. Valtion toimitilojen suojaus on porrastettu neljään kategoriaan ylimmästä alimpaan seuraavasti:

I Täyssuojaus,
II Erityissuojaus,
III Tehostettu perussuojaus ja
IV Perussuojaus.

Valtion rakennusten turvallisuusjärjestelyjen peruslähtökohtana on alueellinen osastointi, joka perustuu ns. *kehäajatteluun* eli osastot muodostavat turvallisuusteknisesti jaoteltuja vyöhykkeitä. Rakennusten turvallisuusjärjestelyihin liittyviä muita toimenpiteitä ovat rakenteellinen suojaus, tekniset valvontalaitteistot ja henkilöstön suorittama valvonta.

2.2.5. *Tietoliikenneturvallisuus*

Tietoliikenneturvallisuudella *(Communications Security)* tarkoitetaan niitä televiestintään liittyviä toimenpiteitä, joilla pyritään varmistamaan tietoverkoissa välitettävien tietojen luottamuksellisuus, eheys ja käytettävyys. Päämääränä on tietoliikennelaitteiden fyysinen turvallisuus, viestien alkuperäisen koskemattomuuden ja luottamuksellisuuden turvaaminen, lähettäjien, vastaanottajien ja pääteolioiden todentaminen sekä väärinreitittymisen estäminen.

Tietoliikenneturvallisuuteen katsotaan kuuluvan asiat, jotka koskevat tietoliikennelaitteiden (laitteisto, ohjelmisto, verkko) kokoonpanoa, luettelointia, muutosten valvontaa, ylläpitoa ja ongelmatilanteista ilmoittamista (laadunvalvontaa), käytön valvontaa, verkon hallintaa, pääsynvalvonnan turvallisuusominaisuuksia, turvallisuuden kannalta merkityksellisten tapahtumien tallentamista, paljastamista ja tarkkailua sekä tietoliikenneohjelmien testausta ja hyväksymistä.

Tietoliikenneturvallisuus on luonnollisesti osa hajautettujen järjestelmien kokonaisuutta eikä sitä käytännössä voida käsitellä erillään muusta turvallisuudesta.

Tietoverkkojen yleistyessä on tietoliikenneturvallisuuden merkitys kasvanut huomattavasti. Erityisesti se korostuu organisaatioiden välisen tiedonsiirron (OVT, *Electronic Data Interchange,* EDI) laajentuessa. Turvallisuustasojen määrittämistä onkin pidettävä lähiajan tärkeänä kehittämistavoitteena.

2.2.6. *Laitteistoturvallisuus*

Laitteistoturvallisuudella *(Hardware Security)* tarkoitetaan tietojenkäsittely- ja tietoliikennelaitteiden kokoonpanoon, kunnossapitoon ja laadunvarmistukseen liittyviä turvallisuusominaisuuksia.

Laitteistoturvallisuusominaisuudet voidaan ohjelmistoturvallisuusominaisuuksien tavoin luokitella viiteen alaryhmään:

a) Laitteiston tunnistamisominaisuudet,
b) Eristämisominaisuudet,
c) Pääsynvalvontaominaisuudet,
d) Tarkkailu- ja paljastamistoimenpiteet ja
e) Laadunvarmistustekniikat.

Laitteistoturvallisuuteen voidaan lukea myös ns. hajasäteilysuojaus ja suojaus elektromagneettista pulssia vastaan. Osittain nämä kuuluvat myös edellä mainitun fyysisen turvallisuuden piiriin.

Laitteiston tunnistamisominaisuudet tarjoavat yleensä ohjelmistoa tehokkaamman turvallisuuden. Eristämisominaisuudet estävät oikeudettoman käytön, pääsynvalvonta sallii sen oikeutetuissa tilanteissa. Tarkkailu- ja paljastamistoimenpiteet voidaan asentaa myös laitteistoon. Kahdennetut prosessorit, ylimääräinen varakapasiteetti, ns. korvaava bitti, redundanssikomponentit[27] ja piirit samoin kuin virheidenkorjauslogiikka ovat myös laitteistoturvallisuutta. Laadunvarmistus- ja valvonta *(Quality Assurance and Control)* vaikuttavat oleellisesti paitsi tuotevioista aiheutuviin kustannuksiin myös tietojen, järjestelmien ja palveluiden luottamuksellisuuteen, eheyteen ja käytettävyyteen.[28]

2.2.7. *Ohjelmistoturvallisuus*

Ohjelmistoturvallisuudella *(Software Security)* tarkoitetaan tietojenkäsittelylaitteistojen käyttöjärjestelmien ja sovellusohjelmien samoin kuin tietoliikennejärjestelmien ohjelmien turvallisuusominai-

---

27 Redundanssilla tarkoitetaan informaation luotettavuutta varmistavaa ylimäärää.

28 On arvioitu, että monesti jopa 30-40 %:iin organisaation tietoteknikkabudjetin loppusummasta nousevia projektien hukkakuluja on mahdollista vähentää yli puolella asianmukaisen turvallisuussuunnittelun avulla. Ks. RCMP EDP-Security Bulletin, April 1992 s. 1 ss. *"Achieving Quality Services with Security"*.

suuksia. Ohjelmistoturvallisuuteen sisältyy tärkeänä komponenttina laadullinen luotettavuus.

Tätä tietoturvallisuuden keskeistä aluetta (ohjelmathan vasta saavat tietokoneet suorittamaan peräkkäisiä alkeistoimintojen jonoja eli käsittelemään tietoja) voidaan laitteistoturvallisuuden tavoin lähestyä ohjaus- ja sovellusohjelmien osalta seuraavien viiden alaryhmän puitteissa:

a) Ohjelmiston tunnistamisominaisuudet,
b) Eristämisominaisuudet,
c) Pääsynvalvontaominaisuudet,
d) Tarkkailu- ja paljastamistoimenpiteet ja
e) Laadunvarmistustekniikat.

Turvallisuusominaisuuksia ovat vastapuolen tunnistus, käyttöoikeuksien hallinta, eheyden varmistaminen ja lokien pitäminen. Luotettava toiminta edellyttää ohjelmien hankkimista luotettavilta toimittajilta, vain virusvapaiden ja kopiointisuojaamattomien ohjelmien käyttöä, kunnollisen dokumentaation ylläpitoa ja joissain tapauksissa myös lähdekoodin hallussapitoa.

Ohjelmiston tunnistamisominaisuuksien osalta käyttöjärjestelmä on avainasemassa ja sen tulee pystyä yksilöidysti tunnistamaan kaikki tietomodulit, prosessit, resurssit ja käyttäjät. Ohjelmiston eristämisominaisuudet täydentävät laitteiston vastaavia ominaisuuksia.

Pääsynvalvonta toteutetaan mm. käyttöoikeusluetteloiden ja -taulukoiden avulla. Tarkkailu- ja paljastamistoimenpiteet ovat nykyisissä suurkonejärjestelmissä pääasiassa käyttöjärjestelmän ominaisuuksia, joita täydentävät lokien analysointiin tarkoitetut apuohjelmat.

Laadunvarmistus- ja valvonta vaikuttavat laitteistojen tavoin oleellisesti paitsi ohjelmistovioista aihetuviin kustannuksiin myös tietojen, järjestelmien ja palveluiden luottamuksellisuuteen, eheyteen ja käytettävyyteen. Ohjelmien uudelleenmuokkaus ja ennen kaikkea tuottavuuden lasku ennen kuin järjestelmä toimii kunnolla voi aiheuttaa huomattavia taloudellisia vahinkoja.[29]

[29] Oikeuskansleri Jorma S. Aallon huhtikuussa 1992 antaman päätöksen mukaan verohallitus ei noudattanut tarpeellista varovaisuutta ryhtyessään uudistamaan elokuussa 1988 verotuslaskennan tietosysteemejä. Riskien hallitsemattomuuden takia uudistustyö viivästyi, mikä on pitkittänyt verotuksen valmistumista jo kahtena vuotena.

Jo ohjelmien rakentaminen sisältää melkoisen määrän riskejä, joiden toteutuminen on jopa todennäköisempää ja yleisempää kuin muut vahingot. Ohjelmistot eivät valmistu määräaikana, ne sisältävät virheitä, jotka aiheuttavat suuria taloudellisia menetyksiä tai haittaa viraston tai laitoksen ns. imagolle. Ohjelmistot saattavat valmistuessaan olla rakenteeltaan sellaisia, että niiden ylläpito ja kehittäminen jatkossa vaatii enemmän resursseja kuin taloudellisesti olisi kannattavaa.

Sekä suurkoneille että mikroille on markkinoilla runsaasti erityisiä turvallisuusohjelmistoja, joiden ominaisuudet riittävät varsin pitkälle. Myös mikrojen käyttöjärjestelmiin ja verkkopalvelimiin sisällytetään nykyään yhä enemmän välttämättömiä turvallisuusominaisuuksia ja toimintoja. Varusohjelmien ohjelmoinnissa pyritään kaikissa käyttöympäristöissä kiinnittämään turvallisuuteen entistä suurempaa huomiota.

2.2.8 Tietoaineistoturvallisuus

Tietoaineistoturvallisuudella *(Data Security)* tarkoitetaan asiakirjojen, tietueiden ja tiedostojen tunnistamista ja turvallisuusluokitusta sekä tietovälineiden hallintaa ja säilytystä niiden kaikissa eri käsittelyvaiheissa luomisesta hävittämiseen saakka.

Tietoaineistoturvallisuuden käsite kattaa siten sekä perinteiset että tietotekniikan kehityksen mukanaan tuomat uudet asiakirjatyypit. Tietovälineet ovat kaikki, olipa sitten kysymys sähkömagneettisesta tai optisesta tallennusmuodosta, tarkemmin ajatellen oikeudellisessa mielessä aina olleet *asiakirjoja* eli *juridisesti relevantteja selityksiä.*

Asiakirjan ja teknisen tallenteen yhteisnimityksenä on julkisuuslainsäädännön uudistamisen yhteydessä kuitenkin tarkoituksena ottaa käyttöön ilmaisu *tallenne*. Tästä seuraa, että nykyisten ilmaisujen asiakirjajulkisuus ja asiakirjasalaisuus sijasta tullaan käyttämään käsitteitä tallennejulkisuus ja tallennesalaisuus. Vastaavasti tullaan puhumaan tallenteen julkisuudesta ja tallenteen salassapidosta. Viranomaisen tallenteet jakautuvat julkisuuslainkin mukaan julkisiin, ei-julkisiin ja salassa pidettäviin tallenteisiin.[30]

[30] Ks. tarkemmin julkisuustoimikunnan mietintöä julkisuuslainsäädännön uudistamisesta (Komiteanmietintö 1992:9), joka sisältää ehdotuksen hallituksen esitykseksi Eduskunnalle julkisuuslaiksi ja eräiksi siihen liittyviksi laeiksi.

Julkisuustoimikunnan työn tavoitteena on ollut julkisuuden lisääminen, julkisuuden ja sen poikkeusten välisten rajojen selkinnyttäminen sekä julkisuulainsäädännön käsitteiden selkiinnyttäminen ja yhdenmukaistaminen. Julkisuuslainsäädännössä ei kuitenkaan ole otettu tai voitukaan ottaa kantaa varsinaiseen asiakirjojen (tallenteiden) turvallisuusluokitukseen siinä mielessä kuin se nykyään yleensä tietoturvallisuuden suhteen kehittyneissä maissa ymmärretään.

Asiakirjojen (informaation) turvallisuusluokituksella tarkoitetaan esim. Norjassa ja Kanadassa tietoaineiston jakoa paitsi julkiseen ja ei julkiseen, myös ei-julkisen materiaalin jakoa täsmällisemmin siten, että muodostetaan jälkimmäisen osalta kaksi perusryhmää:

- Salassa pidettäviksi (arkaluonteisiksi) luokitellut tiedot ja asiakirjat (Beskyttelsegradert Information, Information *Designated* as Sensitive) ja

- Valtion turvallisuuden vuoksi luokitellut tiedot ja asiakirjat (Sikkerhetsgradert Information, Information *Classified* in the National Interests).

Ensimmäiseen *Designated*-ryhmään kuuluvia salassa pidettäviä (arkaluonteisia) tietoja ovat esimerkiksi yksityisen henkilökohtaisia oloja (Privacy) koskevat tiedot ja asiakirjat. Toiseen *Classified* -ryhmään sisältyy esim. maanpuolustusta ja turvallisuusviranomaisten toimintaa koskevaa tietoaineistoa.

Suomalaisen tietoaineistoturvallisuuden säännöksistä on tärkein vuonna 1975 annettu valtioneuvoston päätös eräiden salassa pidettävien asiakirjojen käsittelystä.[31] Sen määräykset koskevat perinteisten paperiasiakirjojen lisäksi myös karttoja, piirroksia, kuvia, filmejä, ääninauhoja ja muita niihin verrattavia eli siis myös laajasti tulkittuna nykyisiä tietovälineitä. Valtioneuvoston määräysten mukaisesti asiakirjat on varustettava merkinnällä SALAINEN, jos asiakirjan tuleminen asiattoman tietoon saattaa vaikeuttaa valtakunnan ulkopolitiikan tai maanpuolustuksen hoitamista taikka aiheuttaa vakavaa vahinkoa muille kuin edellä mainituille yleisille eduille taikka yhteisöille tai yksityisille. ERITTÄIN SALAINEN merkintää käytetään, jos asiakirjan tuleminen asiattomien tietoon saattaa aiheuttaa vakavaa vahinkoa tai vaaraa valtakunnan turvallisuudelle tai suhteille ulkovaltoihin.

[31] VNp eräiden salassa pidettävien asiakirjojen käsittelystä valtionhallinnossa, Valtioneuvoston kanslia, 27.11.1975, no 1043/140/75 VK-

Yleisten asiakirjojen julkisuudesta annetun lain käsitteistö ei tunnetusti ole erityisen selkeä, joten sitä on syytä eritellä tässä vielä hieman tarkemmin. Edellä olevan nojalla voidaan siis todeta, että perusjakona on kaksi luokkaa: 1. Julkinen ja 2. Ei-julkinen. Jälkimmäinen ryhmä sisältää kuitenkin erään lisäjaottelun, jota ei lakia lukiessa ensin aina huomaa, mutta jolla on ratkaisevan tärkeä merkitys. Asiakirjasalaisuus ja vaitiolovelvollisuus koskevat *salassa pidettäviä* seikkoja. Salassa pidettävät asiakirjat ja seikat eivät kuitenkaan ole identtisiä *SALAISTEN* eli merkinnöin SALAINEN ja ERITTÄIN SALAINEN varustettujen asiakirjojen ja niitä koskevien asioiden kanssa. Salaiset ja erittäin salaiset asiakirjat on pääsääntöisesti luokiteltu niiksi niin meillä kuin muuallakin nimenomaan *kansallisten turvallisuusetujen* vuoksi.

Eroa, joka ei myöskään kovin yleisesti ole kansalaisten tiedossa, selventää tavallinen poliisitutkintapöytäkirja. Se ei ole julkinen (vaan salassa pidettävä) ennen kuin asia on ollut esillä oikeudessa. Mikäli kuitenkin on kysymys esimerkiksi maanpetosjutusta, niin siitä tehty pöytäkirja merkitään SALAINEN-leimalla, eikä se tule julkiseksi, vaikka juttu olisikin ehtinyt vireille hovioikeudessa. Salassa pidettävästäkin jutusta voi tutkinnan johtaja harkintansa mukaan antaa tietoja lehdistölle, mutta tietojen antaminen salaisesta maanpetosjutuissa on huomattavasti rajoitetumpaa. Pöytäkirjan antaminen esimerkiksi lehdistölle täyttää virkarikoksen tunnusmerkistön.

Atk-toiminnan loogista suojausta koskevassa valtiovarainministeriön ohjeessa[32] suositellaan atk-tiedostojen osalta käytettäväksi seuraavaa 4-tasoista asiakirjaluokitusta, joka määrittelee tiedon julkisuuden ja toisaalta salassapidon asteen:

- Julkinen
- Ei-julkinen
- Salainen
- Erittäin salainen

Tämä jako on itse asiassa yhteneväinen edellä esitetyn kansainvälisen Designated ja Classified-jaon kanssa. Ei julkisia salassa pidettäviä (muttei salaisia) Designated-luokan suojaa vaativia tietoja ovat suurin osa vaitiolovelvollisuuden piiriin kuuluvista asioista, esi-

[32] Atk-toiminnan looginen suojaus, Valtiovarainministeriö 14.1.1991 no VM 52/01/91.

merkkinä yksityisyyttä koskevat seikat. Nillä ei kuitenkaan ole mitään tekemistä valtakunnan turvallisuuteen liittyvien intressien eikä *Salaisten* tai *Erittäin salaisten* Classified-luokan tietojen kanssa.

Loogisen suojauksen ohjeessa on katsottu, että virasto- ja laitoskohtaisesti laadittava tietoturvallisuuskäsikirja sisältää tarvittavat ohjeet tietojen ja asiakirjojen ja tiedostojen jakamisesta asiakirjaluokkiin sekä niiden suojaamisesta ja käsittelystä. Asiakirjaluokat, joita erotetaan tavallisesti neljä, mainittiin jo edellä. Näitä tietoja käsittelevät järjestelmät on vielä jaettu *kolmeen suojaluokkaan* siten, että järjestelmä tarjoaa asteittain paranevan suojaustason.

- Luokan 1 suojaustaso vastaa järjestelmille asetettavia minimitasovaatimuksia; järjestelmässä voidaan käsitellä vain ryhmiin julkinen ja ei julkinen kuuluvia tiedostoja

- Luokan 2 vaatimukset täyttävä järjestelmä antaa normaalitilanteeseen tavallisesti riittävän, melko hyvän suojaustason; järjestelmässä voidaan käsitellä myös salaisia tiedostoja, ja

- Luokka 3 takaa jo hyvän suojaustason; järjestelmässä voidaan täten käsitellä aiakaisemmin mainittujen tiedostojen lisäksi myös luonteeltaan erittäin salaisiksi luokiteltavia tiedostoja.

Huomattava kuitenkin on, että *asianmukaisen tietoturvallisuuden tasoa* ei suinkaan voida määritellä pelkästään tietojen luottamuksellisuuden perusteella. Myös *eheys* ja *käytettävyys* vaikuttavat oleellisesti. Esimerkiksi täysin julkisen tiedoston kuten kiinnitysrekisterin osalta on suojaustason oltava hyvä, sillä tietojen oikeellisuus on koko tiedoston käyttökelpoisuuden ydin. Ohjeessa on sen vuoksi kehotettu ottamaan tietoturvallisuuskäsikirjaa laadittaessa huomioon myös organisaatiokohtaisesti vaihteleva toiminnan ja tietojen suojaustarve.

Tietoaineistojen fyysisen suojauksen osalta vuodelta 1989 olevassa ohjeessa turvallisuusnäkökohtien huomioon ottamiseksi valtion toimitiloissa[33] suositellaan seuraavaa:

[33] Ohje turvallisuusnäkökohtien huomioon ottamiseksi valtion toimitiloissa, VM:n kirje rakennushallitukselle 12.12.1989, No 4/04/84. - Ohjeen tunnettavuus on käytännössä voitu todeta jääneen eräissä tapauksissa vähäiseksi.

IV *Perussuojaus*

Suojattaville asiakirjoille ja teknisille tallenteille varataan arkistomääräysten mukaiset säilytystilat keskitetysti. Työtiloihin tarvittavat lukittavat irtokalusteet hankkii käyttäjä tarpeen mukaan.

III. *Tehostettu perussuojaus*

Suojattavien asiakirjojen ja teknisten tallenteiden tilat varustetaan tarvittaessa rikosilmoitinlaitteistolla.

II. *Erityissuojaus*

Suojattavien asiakirjojen ja teknisten tallenteiden säilytykseen varataan palo- ja murtosuojatut tilat.

I. *Täyssuojaus*

Teknisten tallenteiden ja suojattavien asiakirjojen säilytystilat varustetaan kulunvalvontalaitteistolla ja rikosilmaisimilla.

2.2.9. Käyttöturvallisuus

Käyttöturvallisuudella *(Operations Security)* tarkoitetaan henkilöstön turvallisia käyttöperiaatteita, käyttöympäristöön ja varsinaisen tietojenkäsittelyyn turvallisuuteen vaikuttavien tapahtumien valvontaa sekä toiminnan jatkuvuuden turvaamiseen liittyvien menettelyjen käyttöä.

Käytön jatkuvuus varmistetaan vahinkoja rajoittavan toipumissuunnitelman (esim. virastojen yhteinen varakeskus) avulla. Ilman asianmukaista dokumentointia ainoastaan harvat pystyvät käyttämään järjestelmää, joten sen ylläpito käyttöturvallisuuden kannalta on yleensäkin merkittävää. Asianmukainen pääsynvalvonta edellyttää lokitietojen suojaamista sekä säännöllistä erittelyä ja ryhtymistä näin paljastuneiden tapahtumien aiheuttamiin vastatoimiin. Käyttöturvallisuuteen kuuluvat myös seuraavassa erikseen selostetut menettelyt.

Tehtävien kahdentamisen (Duplication of Duties) periaatteen mukaisilla varahenkilöjärjestelyillä vältetään atk-tehtävien avainhenkilöriskejä. Sijaisuudet merkitään toimenkuviin ja määritellään työjärjestyksissä. Sijaisuusjärjestelyt vaativat suunnitelmallista koulu-

tusta ja tehtäväkiertoa sekä ajan tasalla olevaa dokumentointia. Samoin on huolehdittava tavanomaisesta töiden varamiesjärjestelyistä kesälomien tms. normaalista poikkeavien tilanteiden aikana sekä urakierrosta.

Tehtävien eriyttämisen (Separation of Duties) periaatetta noudatettaessa eliminoidaan mm. vaarallisten työyhdistelmien syntyminen. Taloustoimintojen klassinen vaarallinen työyhdistelmä on ollut se, että kassaa ja kirjanpitoa on hoitanut yksi ja sama henkilö. Usein virastossa tai laitoksessa on vain yksi tiettyyn atk-järjestelmään perehtynyt henkilö. Tällöin on varmistettava se, että muut kontrollit, talousjärjestelmissä lähinnä täsmäytykset, ovat niin kattavat, ettei ns. vaarallisesta työyhdistelmästä aiheudu vahinkoja. Atk-ympäristössä tällainen yhdistelmä syntyy, jos atk-suunnittelijalle on annettu ohjelmointityönsä lisäksi mahdollisuus osallistua tuotantoon eli ajojen suorittamiseen. Käyttötehtäviä voidaan eriyttää myös siten, että tiettyjä arkaluonteisia, erityistä luotettavuutta vaativia töitä tehdään eri vuoroissa.

Tehtävien kohdennettavuus (Accountability) on eräs tärkeimpiä käyttöturvallisuuden periaatteita. Se on usein määritelty sellaisen tiedoston olemassaoloksi, jonka avulla voidaan todentaa henkilö, joka on suorittanut tietyn toiminnon (esim. tiedoston päivityksen tai turvallisuusrikkomuksen) niin, että vastuu tuosta toiminnosta on yksilöitävissä.[34]

Atk-tarkastajilla on kohdennettavuuteen liittyen oma ns. *kirjausketjun (Audit Trail)* käsiteensä. Sillä tarkoitetaan alkutositteiden, syöttötietojen ja tulosteiden aukotonta ketjua, jonka avulla on mahdollista jäljittää yksittäisen tiedon käsittelyvaiheet.[35]

---

[34] Kohdennettavuus on käyttöturvallisuuden kannalta ratkaiseva ominaisuus esim. tietokoneiden vieraisiin tarkoituksiin käytön torjumiseksi tai kavallusten ja väärennysten estämiseksi. Esimerkiksi Ruotsissa jokin aika sitten tapahtuneessa 53 miljoonan kruunun anastuksessa tietokonenauhan tilitietoa muuttamalla kohdennettavuus ei sisältynyt arvopaperikeskuksen *(Värdepappercentralen)* tietojärjestelmän käyttöperiaatteisiin. Tämän operatiivisen turvallisuuden heikkouden, *kohdennettavuuden*, puutteen vuoksi juttua ei voitu koskaan selvittää, vaan jouduttiin vaivaamaan satoja henkilöitä epäiltyjen piiriin kuuluvina. Ainoastaan vähäinen osa rahoista saatiin takaisin. Osittain tämän tapauksen vuoksi suomalaiseen arvo-osuusjärjestelmälakiin osattiin vuonna 1991 ottaa sen 15 §:ään asianmukainen tietoturvallisuusmääräys.

[35] Kirjanpitolakimme edellyttää visuaalista kirjausketjua (KPL 5 §:n 3 mom., KPA 11 §:n 1 mom.). Kirjausketjun säilyttämistä atk-ympäristössä voidaan valvoa mm. tietueketjujen eheyttä valvovilla ohjelmilla. Kirjanpitolautakunta on lokakuussa 1990 vahvistanut ohjeet koneellisten menetelmien käytöstä. Ohjeiden toisessa osassa määrätään kirjausketjujen sisällöstä ja rakenteesta. Kirjausketjuun kuuluva täsmäytyspakko sinetöi kirjanpidon muuttumattomuuden ja sen, että voidaan visuaalisesti varmistaa eri tietojärjestel-

Käyttöoikeuksien hallinta (System Access Authorization) on sekin käyttöturvallisuuden keskeisimpiä alueita. Pääsy kaikkiin tietoihin ja järjestelmiin tulee olla asianmukaisen pääsynvalvonnan kontrolloima. Tietojen ja järjestelmien käyttöoikeudet ja -valtuudet on määriteltävä ja käyttäjät luokiteltava. Periaatteena on pidettävä, ettei kenellekään anneta sellaisia käyttöoikeuksia, joihin hänellä ei ole toimenkuvansa nojalla järkevää tarvetta (ns. *"Least Privilege"* eli *"Need-to-Know-Principle"*). Käyttörajoituksilla voidaan torjua myös atk-virusten uhkaa kieltämällä ulkopuolelta tuotujen ohjelmien ja diskettien käyttö kokonaan tai rajaamalla se organisaation puolesta järjestetyn tarkastusmenettelyn läpikäyneeseen aineistoon.

Käyttöturvallisuuteen kuuluvat edelleen *varmistukset (Back-up Procedures)*, joilla tarkoitetaan resurssien käytettävyyden ja toimintakyvyn tai tietojen säilymisen häiriöihin varautumista. Käyttötoiminnan varmistamiseen tähtääviä toimia on sekä henkilöstön että laitteiston osalta.

Käytön jatkuvuus varmistetaan vahinkoja rajoittavan *toipumissuunnitelman* avulla. Virastoilla voi olla yhteinen varmistuskeskus, joskin varalaiteyhteistyö on osoittautunut käytännössä hallinnollisesti hankalaksi toteuttaa. Keskeinen kysymys on, kuinka nopeasti varalaitteisto pitää saada käyttöön. Yhdenmukaisella laitekannalla luodaan varakapasiteettia. Poikkeusolojen *valmiussuunnitelmat* tähtäävät ennen kaikkea käyttöturvallisuuden takaamiseen.

Varmistuskopionnin avulla turvataan viraston tai laitoksen toiminnan jatkuvuus tiedostojen tuhoutumisesta aiheutuvilta menetyksiltä. Puutteellinen varmistuskäytäntö voi aiheuttaa huomattavan suuria menetyksiä, pahimmassa tapauksessa jopa sellaisia, ettei tilannetta voida enää millään keinoin palauttaa (ellei kaikista tuhoutuneista tiedostoista ole ajan tasalla olevaa paperitulostusta) tai että rekisterien perustaminen tulee kohtuuttoman kalliiksi.

---

mien tuottamien tietojen oikea ja täydellinen käsittely pääkirjanpidossa. - Hiljakkoin eräässä suomalaisessa alioikeudessa päättyneessä jutussa, jossa oli kysymys 2 miljoonan markan virheellisestä maksusta ja kavalluksesta, tilinumerovirheen syntyä ei voitu kohdentaa. Myös visuaalisessa varmennuksessa oli laiminlyöntejä.
Tuorein uudistus on siirtyminen vuoden 1993 loppuun mennessä kuitittomaan kirjanpitoon. Se perustuu kirjanpitolautakunnan elokuussa 1990 antamaan lausuntoon, jonka mukaan muun muassa erillisistä maksutositteista voidaan luopua ja pankkitapahtumien tositetiedot voidaan välittää asiakkaille tiliotteilla. Tietoturvallisuuden kannalta järjestelmä on oivallinen, koska kirjanpitoa ei ole enää helppoa jälkiä jättämättä hävittää tai muuttaa, koska osa säilyy tallessa pankin tietokoneella seitsemän vuotta.

2.3. Tietoturvallisuusriskien hallinta

2.3.1. Yleistä

Tietojärjestelmät ovat haavoittuvia monista eri syistä johtuen. Tällaisia tekijöitä ovat mm. tietovarojen keskittymisen, järjestelmien monimutkaisuuden sekä mikrojen ja tietoliikenteen nopean kehityksen ja yleistymisen luomat aivan uudet olosuhteet. Keskuslaitteistojen ja mikrotietokoneympäristöjen riskit ovat pääosiltaan samoja. Laitteistojen, ympäristöjen ja käyttötapojen erot aiheuttavat kuitenkin sen, että riskit ja niiden torjunta painottuvat eri tavoin.

Johtajan vastatessa toiminnasta kokonaisuudessaan hänellä tulee olla käsitys myös toiminnan uhkatekijöistä, uhkien toteutumismahdollisuuksista ja niiden aiheuttamista vahingoista. Lyhyesti sanottuna johdon on tunnettava virastonsa ja laitoksensa tietoturvallisuuden yleiskuva ja siihen vaikuttavat tekijät. Riskienhallinta on osa johtamistaitoa.

Voidakseen täyttää tietohallintoasetuksen edellyttämän turvallisuusvelvoitteensa ministeriöiden samoin kuin virastojen ja laitosten johdon on kyettävä pääpiirtein tunnistamaan ja hallitsemaan tietotekniikan lisääntyvään käyttöön liittyvät vaaratekijät. Johdolta edellytetään tietoteknisten omaisuusarvojen sekä niihin kohdistuvien vahinkouhkien (esim. palo- ja vesivahingot, laite- ja ohjelmistovirheet), tuottamuksellisten (esim. käsittelyvirheet) ja tahallisten tekojen (esim. tietomurrot, kavallukset, varkaudet) luonteen yleistä tuntemusta.

Kustannusten ja hyötyjen erittelyssä on otettava huomioon, että asianmukaisen perusturvallisuuden laiminlyönti on kokemuksen mukaan useimmissa tapauksissa ollut syynä vahinkojen syntyyn ja laajuuteen sekä toisaalta mahdollistanut tai ainakin yksinkertaistanut myös rikollisen toiminnan. Vaikkakin täydellinen tietoturvallisuus on jo riskienhallinnan teoriankin mukaan epärealistinen tavoite, niin siedettävä riskinotto on saavutettavissa varsin kohtuullisin ja taloudellisesti hyvin perusteltavissa olevin rahallisin uhrauksin.

2.3.2. Riskianalyysimenetelmät ja skenariotekniikka

Tietoriskien hallintaan on viimeisten 20 vuoden aikana kehitelty eri puolilla maailmaa lukuisia sekä *kvantitatiivisia* että *kvalitatiivisia*

menetelmiä. Niihin liittyvää palvelua on Suomessakin kaupallisesti saatavilla.[36] Kaikki riskianalyysimenetelmät rakentuvat kuitenkin pääosin seuraavien seitsemän toimenpiteen varaan:

1. Tietovarojen tunnistaminen,
2. Arvojen määrittely,
3. Uhkien tunnistaminen,
4. Haavoittuvuuden tunnistaminen,
5. Riskien todennäköisyyden arviointi,
6. Turvallisuustoimenpiteiden valinta ja toteutus,
7. Tietoturvallisuusohjelman seuranta ja korjaaminen.

Eräs varsin yksinkertainen, mutta silti tehokas riskienhallinnan menetelmä, ns. *skenariotekniikka*, on seuraava:

1. Tapahtumien kuvaus,
2. Turvallisuustoimenpiteiden kuvaus,
3. Puutteiden ja heikkouksien erittely,
4. Tapahtuman seurausten kuvaus,
5. Tapahtuman todennäköisyysarvio,
6. Arvio tarvittavista toimenpiteistä ja
7. Ehdotus tarvittavista toimenpiteistä.

Todennäköisyyslaskentaan perustuvat riskianalyysit näyttävät tuottavan hyvinkin luotettavan tuntuisia numeroita. Lähemmin tarkasteltuina nämä numerot kuitenkin paljastuvat pohjautuviksi useimmiten niin epävarmoihin tekijöihin, ettei niitä voida asettaa vakavasti otettavan erittelyn pohjaksi.[37]

---

[36] Tunnetuimpia ovat amerikkalaiset *IBM White Plains Method*, *Livermore Risk Analysis Methodology* (LRAM) ja *Baseline Security Methodology* (SRI), ranskalainen *Marion* ja ruotsalainen valtionhallinnon ja liike-elämän yhdessä kehittämä *Security By Analysis*, aikaisemmin nimellä Sårbarhetsnalys (SBA). *Pohjola-Yhtiöillä* on oma tietoriskien peruskartoitusmenetelmänsä, minkä lisäksi Suomessa on kehitetty *Tuplatiimiprosessi*-niminen systeemi. *Euroopan Yhteisön* tammikuussa 1992 julkistettuun laajaan INFOSEC'92 projektiin sisältyy osana hanke, jolla pyritään Eurooppalaisen tietoturvallisuusriskien hallintastrategian luomiseen yhteistyössä amerikkalaisten, kanadalaisten ja kansainvälisen standardisoimisjärjestön vastaavien projektien kanssa.

[37] Numeroiden epävarmuuteen on erityisesti kiinnittänyt huomiota Suomessakin useita kertoja vieraillut tietoturvallisuusalan tunnetuin auktoriteetti, kalifornialainen *Donn B. Parker (Stanford Research Institute, SRI)*.

Laskennan arvoa ei luonnollisestikaan ole syytä kokonaan kieltää. Lähinnä kysymykseen tulevat keskeytystyyppiset, taajaan toistuvat vahingot (esim. sähkövirran saannin tai tietoliikenteen katkokset), joiden suuruus ja frekvenssi voidaan tuntea. Sensijaan erilaisten tietotekniikkarikosten, esimerkiksi kavallusten, esiintymistodennäköisyys jossain nimenomaisessa ympäristössä on perin epävarmalla pohjalla, sillä se riippuu liian monista ennustamattomista tekijöistä. Tilaisuus voi yleisen elämänkokemuksen mukaan tehdä varkaan, mutta on virheellistä väittää todennäköisyydeksi jotain tiettyä numerollista suuretta.

Viraston tai laitoksen johdon kannalta on loppujen lopuksi tärkeintä huomata, että *päätöksenteon pohjaksi riittää käytännössä kuitenkin varsin yksinkertaisin apuvälinein tehty toiminnan erittely*. Tällä tavoin päästään alkuun ja havaitaan tietoturvallisuuden merkitys kokonaistoiminnan kannalta. Samalla säästetään aikaa ja rahaa myös tarvittavien perussuojaustoimenpiteiden toteuttamiseen.