Pierādījumu saglabāšanas principi IT vidē notikušos noziegumos

Valsts policijas, Galvenās kriminālpolicijas pārvaldes
Ekonomisko noziegumu apkarošanas pārvaldes 4.nodaļa
(kibernoziegumu apkarošana un intelektuālā īpašuma
tiesību aizsardzība)

Elektroniskie pierādījumi

2001.gada 23.novembra Eiropas Padomes Konvencijas par kibernoziegumiem (*Convention on cybercrimes*) normas par elektronisko pierādījumu procesuālo regulējumu tika iestrādātas jaunajā Kriminālprocesa likumā.

Kā vienu no pirmajiem jautājumiem, ko reglamentē EP Konvencija par kibernoziegumiem, ir procesuālie jautājumi par pierādījumu elektroniskā formā meklēšanu, saglabāšanu, iegūšanu, vākšanu un pārtveršanu.

Pierādījumu veidi

- liecības (Kriminālprocesa likums 131.pants)
- eksperta vai revidenta atzinums (KPL 132.pants)
- kompetentās institūcijas atzinums (KPL 133.pants)
- lietiskais pierādījums (KPL 134.pants)
- dokuments (KPL 135.pants)
- elektroniskie pierādījumi (KPL 136.pants)
- operatīvās darbības pasākumos iegūtās ziņas (KPL 127.p.3.d.)
- ziņas par faktiem (KPL 137.pants), kuras nostiprinātas izmeklēšanas darbību protokolos vai fiksētas citās Kriminālprocesa likumā noteiktajās formās

Pierādījumu veidu savstarpējās saistības!!!

Šī konvencija paredz nacionālajā tiesību aktā atsevišķi reglamentēt iespējas veikt tādas kriminālprocesuālās darbības:

- uzkrāto datu operatīva (jeb paatrināta) saglabāšana (*expedited preservation of stored computer data*) nodrošinoties pret datu nozaudēšanu vai izmainīšanu;
- ražošanas uzdevums jeb pieprasījums (*production order*) pakalpojumu sniedzējam vai citai personai, kuru kontrolē ir tādi dati par lietotājiem un viņu identifikāciju un kas nav datu plūsma vai satura dati;
- uzglabāto datu meklēšana un pārņemšana (jeb iegūšana) (*search and seizure of stored computer data*);
- datu plūsmas vākšana reālā laikā (*real-time collection of traffic data*);
- satura datu pārtveršana (*interception of content data*) jeb noklausīšanās.

Elektroniskie pierādījumi

- Ziņas par faktiem, kurām ir nozīme kriminālprocesā
- Kas tieši vai netieši var apstiprināt kriminālprocesā pierādāmo apstākļu esamību vai neesamību,
- Ko procesa virzītājs jeb cita kriminālprocesā iesaistīta persona var izmantot savas pozīcijas pamatošanā un pārliecināšanā
- Var apstrādāties, uzglabāties un pārraidīties elektroniskajā formā
- Atšķirībā no pierādījumu „tradicionālās" izpratnes var būt vienlaikus vairāku personu lietošanā un uzglabāšanā, var būt viegli pārraidīta pāri valsts robežām, viegli grozīta, nokopēta, izdzēsta vai īpaši aizsargāta (piemēram, šifrēta).

Elektroniskie pierādījumi

Šāda situācija prasa atbilstošu, adekvātu un līdzsvarotu procesuālo reglamentāciju šādu ziņu nostiprināšanai un izmantošanai, ievērojot valsts suverenitātes, cilvēktiesību un brīvību aizsardzības intereses, kā arī abstrahējoties no kādas noteiktās tehnoloģijas sasaistīšanas ar tiesību normu, reglamentējot tikai tiesiskos aspektus.

Elektronisko pierādījumu definīcija

- Kriminālprocesa likuma 136.pants

- Par pierādījumu kriminālprocesā var būt ziņas par faktiem elektroniskas informācijas formā, kas tiek apstrādāta, uzglabāta vai pārraidīta ar automatizētas datu apstrādes ierīcēm vai sistēmām

Elektronisko pierādījumu veidi

- abonenta jeb pakalpojuma pasūtītāja identifikācijas informācija („*subscriber information*”)
- datu plūsma jeb ar pārraidi saistīti dati („*traffic data*”)
- satura dati jeb abonenta/pasūtītāja elektroniskā korespondence („*content data*”) – komunikācijas satura dati, kas pārraidīti ar datorsistēmas palīdzību – KPL 12.panta 3.daļa – tikai ar izmeklēšanas tiesneša piekrišanu!!!

Elektronisko pierādījumu izmantošanas problemātika kriminālprocesā

- E-pierādījumu pieļaujamības prasības – ziņu ieguvē nevar būt pieļauts kaut mazākais defekts
- Ziņas ir īpaši jūtīgas pret to grozīšanu un nozaudēšanu
- Procesuālās iegūšanas un nostiprināšanas formas pārkāpums iespaido šo ziņu integritāti (veselumu) līdz ar to ir nepieļaujams
- Elektronisko pierādījumu integritāte, pieejamība un konfidencialitāte ir obligātas šī pierādījumu veida īpašības, kas visā izmeklēšanas gaitā ir speciāli jānodrošina.

Elektronisko pierādījumu nostiprināšanas pamatprincipi (APCO labās prakses rekomendācijas)

- Neviena procesuāli pilnvarotas personas darbība nedrīkst izraisīt izmaiņas datos, kas tiek glabāti datorā vai citā datu nesējā (piemēram, ieslēdzot datoru vai strādājot ar ieslēgtu datoru tiek veiktas izmaiņas datnēs)
- Apstākļos, kad procesuāli pilnvarota persona uzskata par svarīgu piekļūt oriģināldatiem, šai personai ir jābūt pietiekami kompetentai (zināšanas un praktiskā pieredze) tā rīkoties un jābūt spējīgai paskaidrot savu darbību cēloņsakarību un izmaiņas.
- Pierakstīt visu, kas tiek veikts. Veicot darbības ar elektroniskiem pierādījumiem ir būtiski nodrošināt auditācijas pierakstus vai citus aprakstus, kuros tiks detalizēti paskaidroti visi procesi, kas tika pielietoti attiecībā uz pierādījumiem.
- Procesa virzītājs ir atbildīgs par šo principu piemērošanu un ievērošanu izmeklēšanā.

Elektronisko pierādījumu integritāte / nemainīgums

- Pamatprasība un pamatīpašība
- Tiek nodrošināta visās kriminālprocesa stadijās no e-pierādījumu iegūšanas brīža līdz attiecību taisnīgam noregulējumam
- Novērš šaubas par kādas iesaistītas personas ļaunprātīgu rīcību
- Tiek nodrošināta ar kriptogrāfiskās kontrolsummas (jeb *hashsum*) palīdzību

HASHSUM vai kriptogrāfiskā kontrolsumma

- Fiksēta izmēra atskaites aprēķins
- Elektroniskais "pirkstu nospiedums"
- Datnes (faila) integritāte tiek pārbaudīta aprēķinot un vēlāk salīdzinot kontrolsummu
- Visizplatītākie algoritmi – MD5 un SHA1

MD5

- *Message Digest Algorithm*
- 128-bit (16-byte) jaucējvērtība (*hash value*)
- 32 heksadecimālcipari

```
MD5("The quick brown fox jumps over the lazy dog")
= 9e107d9d372bb6826bd81d3542a419d6
```

```
MD5("The quick brown fox jumps over the lazy dog.")
= e4d909c290d0fb1ca068ffaddf22cbd0
```

Kontrolsummas izmantošanas rekomendācijas

- E-pierādījumu iegūšanas (saglabāšanas) brīdī
- Vairāku failu gadījumā sākumā izveidot arhīvu (rar, zip, tar ...), kuram aprēķināt summu
- Ieprotokolējiet rezultātu un summu (datni) saglabājiet kopā ar oriģināldatiem (piemēram, CD-R diskā)
- Vienmēr strādājiet ar kopiju nevis oriģināldatiem!!!

Procesuālās darbības

- Rakstveida pieprasījums izsniegt ziņas elektroniskas informācijas vai dokumenta formā, kas apstrādātas, uzglabātas vai pārraidītas, izmantojot elektroniskās informācijas sistēmas – KPL 190.panta 1.daļa
- Šī darbība paredzēta:

- tādiem datiem, kas nav nekavējoties jāsaglabā (KPL 191.pants)
- datiem, kas nesatur personas korespondence (KPL 12.panta 3.daļa, 192.panta 2.daļa, 220.pants)
- datiem, kas netiek saglabāti saskaņā ar Elektronisko sakaru likuma prasībām - saglabājamie dati (KPL 192.panta 1.daļa)

Elektroniskās informācijas sistēmā esošo datu saglabāšana (KPL 191.pants)

- Kriminālprocesuālais līdzeklis elektronisko pierādījumu „iekonservēšanai”
- Latvijas Republikas robežās esošām sistēmām un ārvalstīs (24/7 kontaktpunkts – VP GKrPP SSB)
- Šādai darbībai seko datu atklāšana (KPL 192.pants) vai starptautiskās krimināltiesiskās palīdzības lūgums
- 30 dienas!

Elektroniskajā informācijas sistēmā esošo datu kontrole (KPL 219.pants)

- Speciālā izmeklēšanas darbība
- Automatizētās datu apstrādes sistēmas (tās daļas), tajā uzkrāto datu, datu vides pārmeklēšana un piekļuve tai, kā arī izņemšana bez šīs sistēmas vai datu īpašnieka, valdītāja vai turētāja ziņas.

Pārraidīto datu satura kontrole (KPL 220.pants)

- Speciālā izmeklēšanas darbība

- Tādu datu pārtveršana, vākšana un ierakstīšana, kuri pārraidīti ar automatizētās datu apstrādes sistēmas palīdzību, izmantojot Latvijas teritorijā esošās sakaru ierīces (turpmāk – pārraidīto datu kontrole), bez šīs sistēmas īpašnieka, valdītāja vai turētāja ziņas.

ADAS satura apskate (KPL 160.panta 6.daļa)

- Automatizētās datu apstrādes sistēmas (tās daļas) apskati parasti uz vietas neveic, bet šo sistēmu (tās daļu) izņem, nodrošinot datu veseluma saglabāšanu neizmainītā stāvoklī.
- Elektronisko pierādījumu nostiprināšanas pamatprincipi!

Paldies par uzmanību!

Aleksandrs Buko

Tālruņa Nr. +371-67208654

buko@vp.gov.lv