Kriminālprocesa

piemērošanas problēmjautājumi,

izmeklējot noziedzīgus nodarījumus

elektroniskā vidē

IT un kriminālprocesa tiesību attīstība

Combating the criminal misuse of information technologies

United Nations, General Assembly resolutions No. 55/63, 2000.; No. 56/121 2001.

Creation of a global culture of cybersecurity

United Nations, General Assembly resolution No. 57/239, 2003.

On attacks against information systems

Proposal of a Directive of the European Parliament and of the Council : Brussels, 30.09.2010.

Impact assessment

Accompanying document to the Proposal of a Directive of the European Parliament and of the Council 'On attacks against information systems'

Starptautisku organizāciju rekomendācijas – OECD, G8, Interpol, Europol...

http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html

IT un kriminālprocesa tiesību attīstība

Konvencija par kibernoziegumiem

Eiropas Padome 23.11.2001. Stājās spēkā 01.07.2004. Latvijā stājās spēkā 01.06.2007.

Papildus protokols par rasisma un ksenofobijas noziedzīgajiem nodarījumiem, kas tiek izdarīti datorsistēmās

Eiropas Padome 28.01.2003. Latvijā stājās spēkā 01.06.2007.

Dalībvalstu tiesību sistēmu harmonizācija:

- kriminalizējamie nodarījumi elektroniskā vidē
- cilvēktiesību aizsardzība (t.sk. korespondences noslēpuma, personas datu aizsardzība)
- izmeklēšanas efektivitātes nodrošināšana (t.sk. veicot slēptas izmeklēšanas darbības)
- 24/7 kontaktcentru (*24/7 High Tech Contact Points*) izveide dalībvalstīs
- starptautiskā sadarbība
- sadarbība ar privāto sektoru (interneta pakalpojumu sniedzējiem, finanšu institūcijām)
- elektronisko pierādījumu izmantošana

IT un kriminālprocesa tiesību attīstība

Nacionālās drošības koncepcija

Pieņemta Saeimā 10.03.2011.

Latvijas prioritātes elektroniskās informācijas telpā esošo apdraudējumu novēršanai:

- tiesiskā regulējuma pilnveidošana
- starpinstitucionālās un starptautiskās sadarbības pilnveidošana
- apdraudējuma identificēšanas un reaģēšanas pilnveidošana
- informācijas tehnoloģiju lietotāju zināšanu pilnveidošana

IT un kriminālprocesa tiesību attīstība

Civilizācijas attīstība:

200'000 g. p.m.ē.

- **pirmatnējā – mednieku / vācēju sabiedrība**

- **agrikulturālā sabiedrība** apt. 8500 g. p.m.ē.

  ganību sabiedrība

  dārzkopju sabiedrība

  tehnoloģiski agrārā sabiedrība 3500 g. p.m.ē. – XVII gs.

- **industriālā sabiedrība** XVIII gs. – XX gs. vidus

pleistocēns

akmens laikmets

paleolīts

mezolīts holocēns

neolīts

bronzas laikmets

dzelzs laikmets

antropocēns

atom-laikmets

kosmosa laikmets

alu zīmējumi

megalīti

mīti

piktogrammas

ideogrammas

rakstība

IT un kriminālprocesa tiesību attīstība

Civilizācijas attīstība:

200'000 g. p.m.ē.

- **pirmatnējā – mednieku / vācēju sabiedrība**

- **agrikulturālā sabiedrība** apt. 8500 g. p.m.ē.
  - ganību sabiedrība
  - dārzkopju sabiedrība
  - tehnoloģiski agrārā sabiedrība 3500 g. p.m.ē. – XVII gs.

- **industriālā sabiedrība** XVIII gs. – XX gs. vidus

- **informācijas sabiedrība** ap 1980.g.

pleistocēns

akmens laikmets
- paleolīts
- mezolīts
- neolīts

holocēns

bronzas laikmets

dzelzs laikmets

antropocēns

atom-laikmets

kosmosa laikmets

informācijas laikmets

alu zīmējumi

megalīti
mīti

piktogrammas
ideogrammas

rakstība

digitālā revolūcija

IT un kriminālprocesa tiesību attīstība

Civilizācijas attīstība:

- **pirmatnējā – mednieku / vācēju sabiedrība**
- **agrikulturālā sabiedrība**

  tehnoloģiski agrārā sabiedrība

- **industriālā sabiedrība**
- **informācijas sabiedrība**

  IT primāra loma – ekonomikā (*knowledge economy*), cilvēces kultūrā, sabiedrības pārvaldē (*e-Democracy*), cilvēku pašapziņā (*digital citizens*), sabiedrības drošībā ...

informācijas laikmets

digitālā revolūcija

... semantic web...

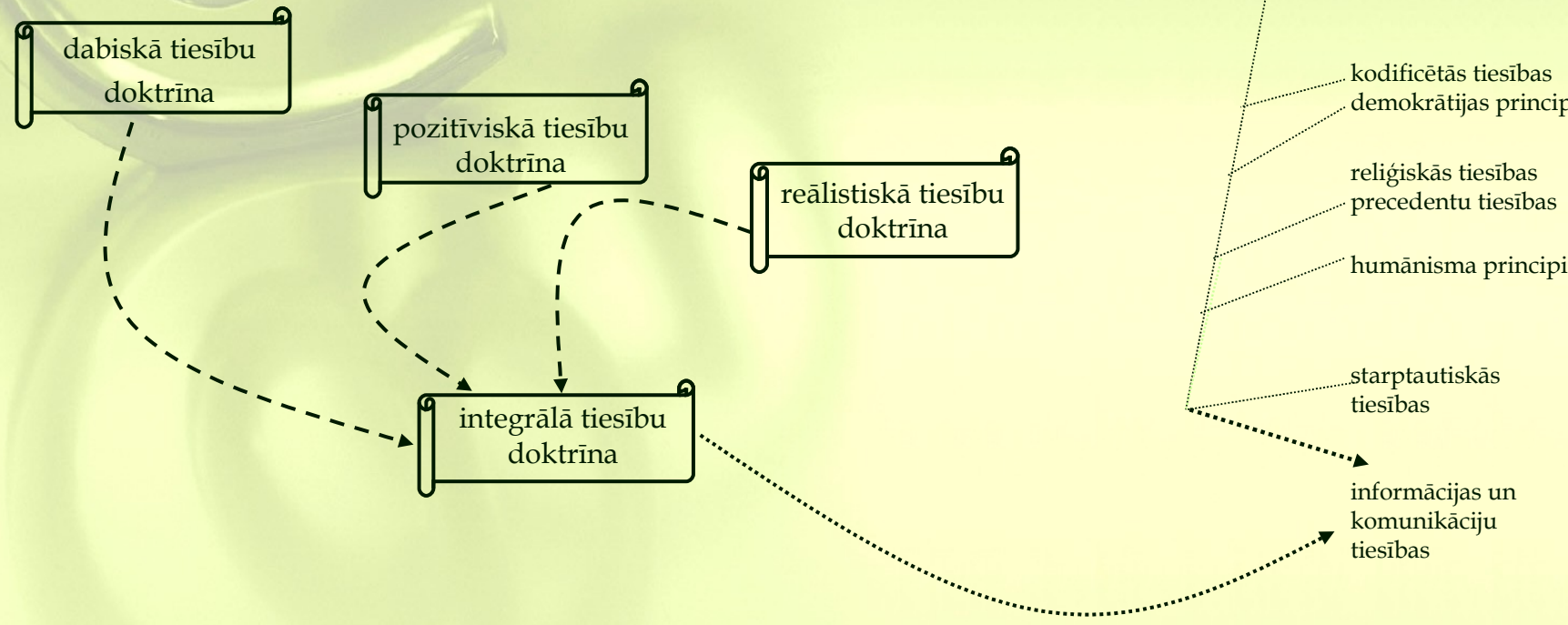
... RoboEarth

IT un kriminālprocesa tiesību attīstība

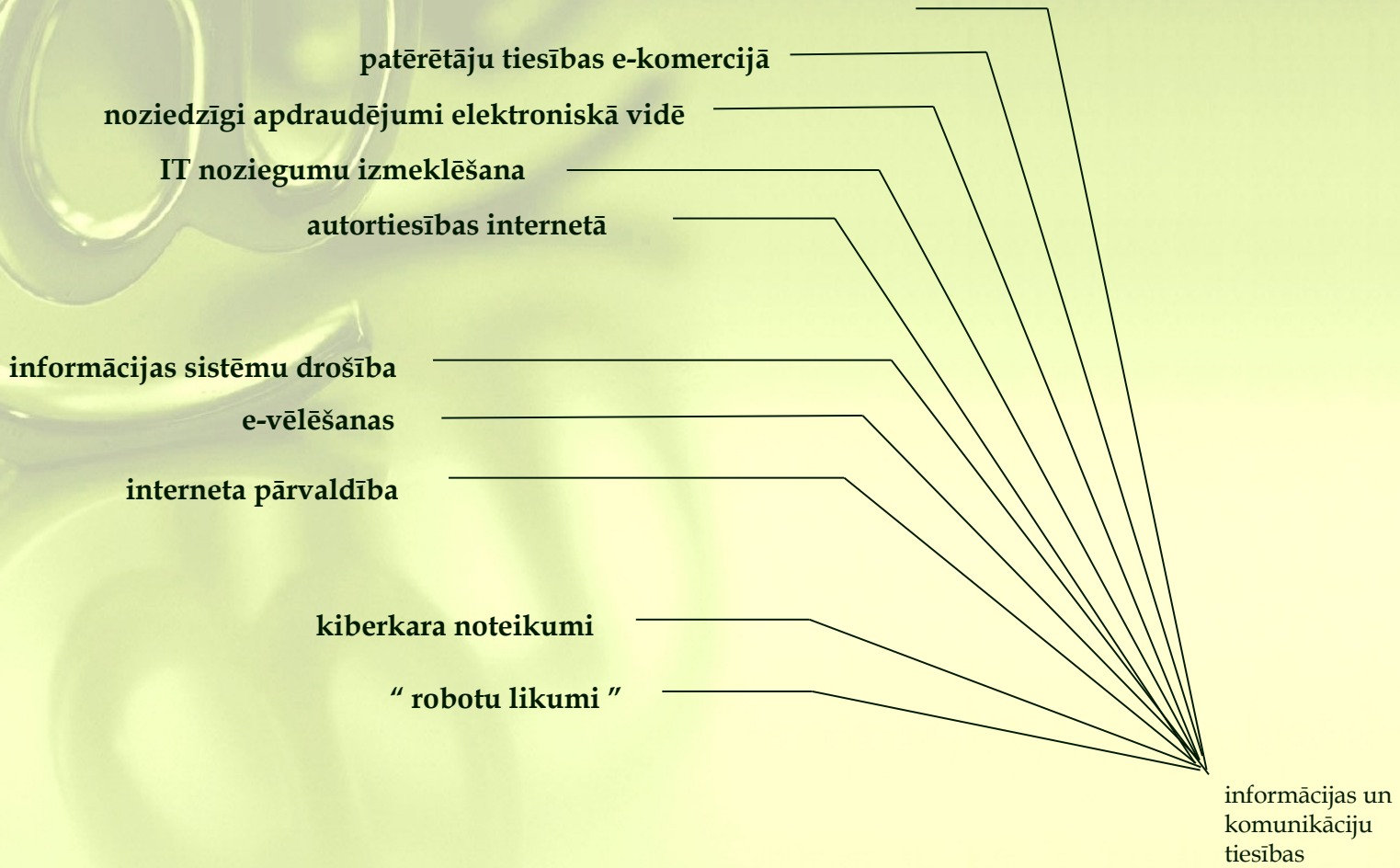
senie laiki	paražu tiesības
antīkie laiki	kodificētās tiesības demokrātijas princip
viduslaiki	reliģiskās tiesības precedentu tiesības
renesance	humānisma principi
modernie laiki	starptautiskās tiesības
informācijas laikmets	informācijas un komunikāciju tiesības

IT un kriminālprocesa tiesību attīstība

Latvijā un visā pasaulē tiesības attīstās – gan tiesību normās, gan juridiskajā praksē ieviešot efektīvus instrumentas sabiedrības un indivīdu interešu aizsardzībai, atbilstīgi vispārējiem tiesību principiem. Vienlaikus attīstās arī juridiskā zinātne, kurā pētī atziņas, kas veidojas tiesisko fenomenu izvērtējumā no dažādu tiesību doktrīnu aspekta. Integrālā tiesību doktrīna sasaista tiesiskās vērtības, tiesību normas, tiesiskos faktus un cilvēku darbības, lai izvairītos no tiesību izpratnes noslēgtības, bet aplūkotu tiesības kā dinamisku un atvērtu juridisko struktūru tiešā saistībā ar juridisko praksi.



IT un kriminālprocesa tiesību attīstība



IT un kriminālprocesa tiesību attīstība

Tiesību pamatprincipi, izmeklējot noziedzīgus nodarījumus

Tehnoloģiskā progresa izaicinājumi, izmeklējot noziedzīgus nodarījumus

IT un kriminālprocesa tiesību attīstība

Tiesību pamatprincipi, izmeklējot noziedzīgus nodarījumus

- likumības princips
- samērīguma princips
- tiesiskās pēctecības princips

Tehnoloģiskā progresa izaicinājumi, izmeklējot noziedzīgus nodarījumus

IT un kriminālprocesa tiesību attīstība

Tiesību <u>pamatprincipi</u>, izmeklējot noziedzīgus nodarījumus

- likumības princips
- samērīguma princips
- tiesiskās pēctecības princips

Tehnoloģiskā progresa <u>izaicinājumi</u>, izmeklējot noziedzīgus nodarījumus

- elektroniskā identitāte / datorizēta dzīves vide
- virtuālā nauda un mantas / virtuālā ekonomika
- kriptogrāfija un steganogrāfija / mākoņskaitļošana
- kiborgi / robotu tīkli / mākslīgais intelekts utt.

Tiesību politikas un juridiskās prakses problēmjautājumi

- kibernoziegumu procesuāla izmeklēšana *vs.* militāra atvairīšana
- "elektroniska policejiskā valsts" *vs.* "kiber-anarhija"
- tīkla monitorings un pierādījumu proaktīva ieguve
- pierādījumu attālināta ieguve
- pierādījumu ieguve ar slēpti instalētu programmatūru
- personas identitāte elektroniskā vidē
- prasība atklāt šifra atslēgu
- elektroniskas informācijas izpētes nosacījumi
- virtuālo noziegumu izmeklēšana

Tiesību politikas un juridiskās prakses problēmjautājumi

- kibernoziegumu procesuāla izmeklēšana *vs.* militāra atvairīšana

2000 – NATO (*bij.Dienvidslāvija*)
2001 – ASV
2007 – Igaunija
2008 – Gruzija
2009 – Dienvidkoreja
2010 – Indija / Pakistāna
2010 – Irāna (stuxnet)
2011 – Izraēla

Ap 120 valstis attīsta iespējas internetu izmantot kā līdzekli uzbrukumiem / pretterorisma pasākumiem.

Kiberkaru var īstenot arī nevalstiskas organizācijas vai atsevišķas personas – "asimetriskie uzbrukumi".

Bukarestes un Lisabonas samitā tika izskatīta 2010.gada NATO Stratēģiskā koncepcija par NATO līguma 5.panta piemērošanu kiberuzbrukumu gadījumos.

Kiberkarš – politiski motivētas sistēmiskas darbības, kas vērstas uz IT kritiskās infrastruktūras apdraudējumu (sabiedrības drošības, loģistikas, enerģētikas, valsts pārvaldes, finanšu sistēmas utt.), kā arī propagandas īstenošanu.

Krimināltiesību aspektā – terorisms, kaitniecība, spiegošana, IS darbības traucēšana, patvaļīga piekļūšana IS utt.

Noziedzīgu nodarījumu izmeklēšana notiek kriminālprocesuālā kārtībā.
To atklāšana un prevencija – kā CERT un IS drošības pārvaldienu tehniskie pasākumi un tiesībsargājošo iestāžu operatīvās darbības pasākumi.

Tiesību politikas un juridiskās prakses problēmjautājumi

- "elektroniskā policejiskā valsts" *vs*. "kiber-anarhija"

Fantastu nosauktās antiutopiskas attīstības pazīmes:

1. Elektroniski identitātes dokumenti: obligāta to izsniegšana un elektroniska reģistrācija.
2. Robežkontrole: datoru pārmeklēšana, prasība atklāt šifrētus datus.
3. Finanšu izsekošana: valsts spēja ievākt un saglabāt visas finanšu transakcijas.
4. Atklātības liegums: krimināsods, ja kāds atklāj, ka valsts pārmeklē šīs personas apstrādātos datus.
5. Kriptēšanas ierobežošana: liegums izmantot kriptēšanas un/vai privātuma līdzekļus (t.sk. anonīmos tīklus).
6. Konstitucionālā aizsardzība: cilvēktiesību aizsardzības juridiska vai praktiska neesamība.
7. Datu uzglabāšanas iespēja: spēja valstī uzglabāt savāktos datus.
8. Datu ievākšanas iespēja: spēja valstij meklēt un ievākt datus, ko tā uzglabā.
9. IPS dati: pienākums interneta pakalpojuma sniedzējiem saglabāt detalizētus datus par klientu aktivitātēm internetā.
10. Telekomunikācija dati: pienākums telekomunikācijas operatoriem saglabāt detalizētus datus par klientu veiktajiem zvaniem un telekomunikācijas tīkla lietošanu.
11. Medicīnas dati: pienākums medicīnas pakalpojumu sniedzējiem saglabāt detalizētus datus par klientiem.
12. Tiesībsargājošo iestāžu pilnvaras: iespēja, veicot kratīšanas, izmantot pārmērīgu spēku (policijas speciālās vienības).
13. *Habeas Corpus*: tiesiska regulējuma neesamība vai neievērošana par to, ka tiesnesis izvērtē apcietinājuma pamatotību.
14. Policijas un specdienestu kompetences nošķiršana: tādas barjeras juridiska neesamība vai neievērošana.
15. Slēpta piekļuve: valsts slēpti veikta elektronisko pierādījumu ieguve no privātiem datoriem.
16. Brīvas pilnvaras: policijas lēmumu pieņemšana bez pilnībā neatkarīga tiesneša rūpīgi veiktas pārbaudes.

Tiesību politikas un juridiskās prakses problēmjautājumi

- tīkla monitorings un pierādījumu proaktīva ieguve

izlūkošanas / pretizlūkošanas / pretterorisma informācijas ievākšana – pārtverot komunikācijas ar ārvalstniekiem

SIGINT (Echelon, Frenchelon, Onyx) / GhostNet / SORM-2 utt.

<u>Konvencija par kibernoziegumiem</u>

29. pants - Uzkrāto datu operatīva saglabāšana
30. pants - Saglabātās datu plūsmas operatīva atklāšana
33. pants - Savstarpējā palīdzība datu plūsmas vākšanai reālā laikā
34. pants - Savstarpējā palīdzība attiecībā uz satura datu pārtveršanu
35. pants - 24/7 tīkls

Pierādījumu ieguve, aizskarot personas cilvēktiesības, pieļaujama vienīgi ar tiesneša atļauju, kur norādīts pamatojums un informācijas ieguves objekts, mērķis, apjoms, veids un periods!

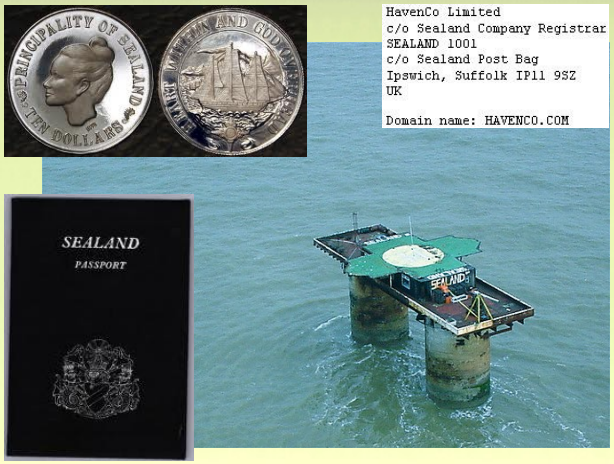
? - *HoneyPot* metode pedofilu atklāšanai internetā

Operatīvās darbības likuma 15.p. Operatīvais eksperiments
Kriminālprocesa likuma 227.p. Noziedzīgas darbības kontrole

Tiesību politikas un juridiskās prakses problēmjautājumi

- pierādījumu attālināta ieguve

ANO aicina visām valstīm tiesiski sadarboties,
lai nepieļautu kibernoziegumiem "drošas debesis" (*safe data haven*).



***cloud computing* !**

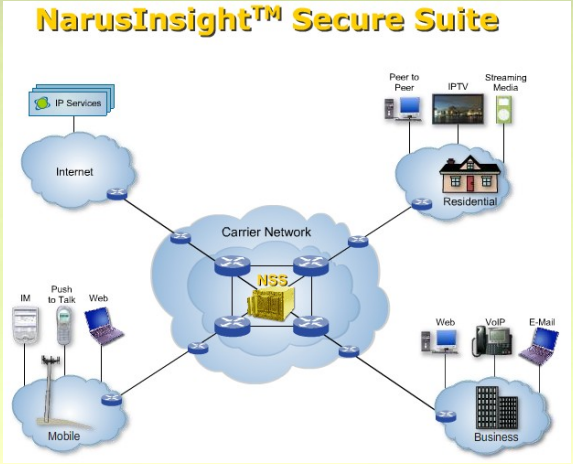
Konvencijā par kibernoziegumiem – teritoriālā jurisdikcija un eksteritoriālā aktīvā jurisdikcija.
krimināltiesībās – arī eksteritoriālā pasīvā jurisdikcija
Universālā jurisdikcija [pagaidām?] netiek attiecināta uz kibernoziegumiem.
Bērnu pornogrāfijas izplatīšana – atkarībā no nodarītā kaitējuma smaguma – var būt atzīta par noziegumu pret cilvēci.
(Starptautiskā krimināltiesa iegūst pierādījumus ar dalībvalstu palīdzību.)

<u>Konvencija par kibernoziegumiem</u>
32. pants - Pārrobežu piekļūšana uzkrātiem datiem ar piekrišanu vai kur tie ir publiski pieejami
Puse var bez citas Puses atļaujas:
b) piekļūt vai saņemt ar tās teritorijā atrodošās datorsistēmas palīdzību uzkrātos datus, kas atrodas citā Pusē, ja Puse saņem likumīgu un brīvprātīgu tās personas piekrišanu, kurai ir likumīgas tiesības atklāt datus Pusei ar attiecīgās datorsistēmas palīdzību.
Krievija nepievienojās Konvencijai, jo šis pants apdraud tās suverenitāti un nacionālo drošību.

2000.gada lieta – par Krievijas hakeriem Gorškovu un Ivanovu, kurus FIB atvilināja uz ASV, kur viņus arestēja, kā arī izmeklētājs patvaļīgi piekļuva viņu serverim Čeļabinskā no datora Sietlā, lai iegūtu pierādījumus par viņu noziegumiem ASV.

Tiesību politikas un juridiskās prakses problēmjautājumi

- pierādījumu ieguve ar slēpti instalētu programmatūru



'Trojas zirgs' vai *'Network forensic tool'* ?

"Bundestrojaner" Quellen-TKÜ jeb Backdoor.Win32.R2D2.a

- VoIP saziņas, t.sk. Skype noklausīšanās
- arī tīkla aktivitātes monitorings, tastatūras datu un ekrānattēlu fiksēšana
- programmas attālināta (caur ārvalstu proxy serveriem) neautorizēta kontrole un funkcionalitātes atjaunošana
- antivīrusa programmatūras neidentificēja (līdz *Chaos Computer Club* publikācijai)

Latvijas Republikas Satversmes 116.p.
Konvencijas par kibernoziegumiem 19., 20., 21.p.
Krimināprocesa likuma 219., 220.p.
Operatīvās darbības likuma 17.p.

Darbības mērķi norādīti Krimināprocesa likuma 211.p. (1) d. vai Operatīvās darbības likums 17.p.

Jānodrošina visu šīs darbības aspektu legalizēšana ar tiesneša atļauju attiecīgajā lēmumā, tai skaitā, ka netiek radītas jebkādas kaitīgas sekas un netiek aizskartas cilvēktiesības vairāk, kā tiesnesis atļāvis.

Krimināllikums
144. Korespondences, pa telekomunikāciju tīkliem pārraidāmās informācijas un citas informācijas noslēpuma pārkāpšanu
241. Patvaļīga piekļūšana automatizētai datu apstrādes sistēmai

Tiesību politikas un juridiskās prakses problēmjautājumi

- personas identitāte elektroniskā vidē

  identifikācija / autentifikācija / autorizācija

  biometriskie dati / I-name

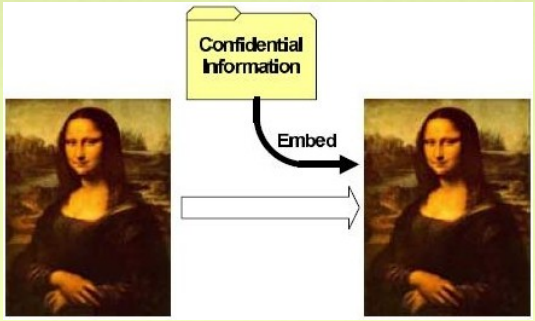
  identitātes slēpšana
  (wardriving, anonymous proxy, TOR...)

  Identitāte – cilvēktiesību aspekts?

  Kāda [autentifikācijas] datu integritātes pakāpe ļauj juridiski identificēt fizisku personu?

Tiesību politikas un juridiskās prakses problēmjautājumi

- prasība atklāt šifra atslēgu



Cilvēktiesību princips – tiesības neliecināt pret sevi.
(aizdomās turētajam/apsūdzētajam)
Vienlaikus – var būt pienākums dot datus (paraugus) izpētei.

Iespējama atšķirīga pieeja privātuma tiesību ierobežošanā:
1) šifrēšanas atslēgu publiska kontrole
2) prasība iesniegt informāciju nešifrētā formā
3) prasība atklāt šifra atslēgu

Francija (3 līdz 5 gadi ieslodzīgumā + 45'000 līdz 75'000 EUR sods)
Austrālija (6 mēn. ieslodzījumā)
Apvienotā Karaliste (2 gadi ieslodzījumā)
Beļģija (6 līdz 12 mēn. ieslodzījumā + 20'000 BEF sods)
Nīderlande (3 mēn. ieslodzījumā)
Indija (7 gadi ieslodzījumā)

http://rechten.uvt.nl/koops/cryptolaw/

<u>Konvencija par kibernoziegumiem</u>
18. pants

Nepieprasa, taču pieļauj dalībvalstīm tādu normatīvo reglamentāciju, kas ļauj pieprasīt informāciju nešifrētā formā.
Taču norāda uz indivīdu tiesībām pielietot šifrēšanu – kā privātuma aizsardzības līdzekli, ko valsts nedrīkst aizliegt.

Aizskarot privātumu, vajadzīga tiesneša atļauja!

Tiesību politikas un juridiskās prakses problēmjautājumi

- elektroniskas informācijas izpētes nosacījumi

pētāmo datu ieguves optimizācija un integritātes verifikācija

[datortehniskās] ekspertīzes metodes validācija

ekspertīžu iestāžu kvalitātes standarti
EN ISO/IEC 17025
ISO 8402 : 1994 -2.18

«Guidelines for best practice in the forensic examination of digital technology», ENFSI, FIT-2005-001, 12.06.2006.

tiesu ekspertu sertifikācija Latvijā / ārvalstīs veiktu ekspertīžu rezultātu novērtēšana

Tiesību politikas un juridiskās prakses problēmjautājumi

- virtuālo noziegumu izmeklēšana

  virtuālā identitāte, virtuālie objekti –
  pastarpinātas, taču reālas [un ilgstošas] darbības rīki

  virtuālo lietu / naudas / spēju vērtība –
  atbilstīgi virtuālās vides nosacījumiem,
  ievērojot arī individuālo investīciju apmēru

  virtuālo tēlu (avataru) integritātes apdraudējumi –
  arī ar morālās traumas raksturu

  virtuālā nozieguma apstākļu izpēte –
  attiecīgās vides modelēšana
  (ekrānattēli ar aprakstu vai pat 3D/4D modelis)

  pierādījumu ieguve par virtuālajiem objektiem –
  pārrobežu un mākoņdatošanas aspekti


28/10/2008 / THE NETHERLANDS

Sentenced for a virtual crime

Japan | law | Netherlands | virtual world

A crime scene in the virtual world, *Second Life*.

Two Dutch youths were sentenced for stealing virtual goods last week, while a Japanese piano player was jailed for killing her virtual ex-husband.

Vai krimināltiesību politika, prevencija – tāda pati, kā reālo noziegumu jomā?