

# Konvencija o kibernetičkom kriminalu

Konvencija definira pojmove, zakonske mjere (na nacionalnoj razini) za pojedine tipove kaznenih djela te pravila o prikupljanju dokaza. Dio Konvencije koji se direktno odnosi na rad računalnog forenzičara su [Članak 19. \(Pretraga i oduzimanje pohranjenih računalnih podataka\)](#), [20. \(Prikupljanje računalnih podataka u realnom vremenu\)](#) i [21. \(Presretanje podataka o sadržaju\)](#).

Konkretni koraci istrage nisu regulirani zakonom no, ako nisu kvalitetno odrađeni, postoji rizik odbijanja tako prikupljenih dokaza na sudu. Ophođenje s dokazima u istrazi je stvar dobre prakse i unutar svake tvrtke postoje vlastita pravila kojih se istražitelji trebaju pridržavati. Jednako tako se pravila razlikuju od države do države te istražitelj treba biti upoznat sa zakonskom regulativom drugih zemalja ako se istraga proširi na inozemstvo.

---

## Dio 4. - Pretraga i oduzimanje pohranjenih računalnih podataka

### Članak 19. - PRETRAGA I ODUZIMANJE POHRANJENIH RAČUNALNIH PODATAKA

1. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi njena nadležna tijela bila ovlaštena izvršiti pretragu ili na sličan način imali pristup:
  - a. računalnom sustavu ili njegovom dijelu, kao i računalnim podacima pohranjenim u njima;
  - b. mediju za pohranu računalnih podataka u kojemu računalni podaci mogu biti pohranjeni na državnom području stranke.
2. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi se osiguralo da – u slučajevima kada njena tijela pretražuju ili na sličan način pristupaju određenom računalnom sustavu ili njegovom dijelu u skladu s točkom (a) stavka 1. ovoga članka, s osnovanom sumnjom da su traženi podaci pohranjeni u drugom računalnom sustavu ili njegovom dijelu na državnom području stranke, a tim se podacima može zakonito pristupiti iz prvog sutava, ili su njemu dostupni – ta tijela budu u mogućnosti hitno protegnuti pretragu ili slično postupanje i na taj drugi sustav.
3. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi ovlastila svoja nadležna tijela za oduzimanje ili osiguranje na neki sličan način računalnih podataka kojima je pristupljeno u skladu s odredbama stavaka 1. ili 2. ovoga članka. Te mjere će uključivati davanje ovlaštenja tijelima da:
  - a. oduzmu ili na sličan način osiguraju računalni sustav, njegov dio ili medij za pohranu računalnih podataka;
  - b. načine i zadrže kopiju tih računalnih podataka;
  - c. održe cjelovitost relevantnih pohranjenih računalnih podataka i
  - d. učine nepristupačnim ili odstrane te računalne podatke iz računalnog sustava kojemu je pristupljeno.
4. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi njena nadležna tijela bila ovlaštena naložiti svakoj osobi koja ima saznanja o funkcioniranju računalnog sustava ili o mjerama poduzetim radi zaštite računalnih podataka u njemu da dade informacije koje su razumno nužne kako bi se omogućilo poduzimanje mjera navedenih u stavcima 1. i 2. ovoga članka.
5. Ovlaštenja i postupci navedeni u ovom članku bit će u skladu s člancima 14. i 15. ove Konvencije.

## Dio 5. Prikupljanje računalnih podataka u realnom vremenu

### Članak 20. – PRIKUPLJANJE RAČUNALNIH PODATAKA U REALNOM VREMENU

1. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi njena nadležna tijela bila ovlaštena u realnom vremenu:

a. prikupiti ili snimiti primjenom tehničkih sredstava na državnom području te stranke, te  
b. primorati davatelja usluga u okviru njegovih postojećih tehničkih mogućnosti da:

i. prikupi ili snimi primjenom tehničkih sredstava na državnom području te stranke ili

ii. surađuje i pomogne nadležnim tijelima da prikupe i snime podatke o prometu u vezi s određenim komunikacijama na svojem državnom području prenesenima pomoću računalnog sustava.

2. Kada stranka zbog uspostavljenih načela svojega unutarnjeg pravnog sustava ne može usvojiti mjere navedene u točki (a) stavka 1., ona može umjesto toga usvojiti zakonske i druge mjere potrebne kako bi se osiguralo prikupljanje ili snimanje u realnom vremenu podataka o prometu vezanih uz određene komunikacije na njenom državnom području primjenom tehničkih sredstava na tom području.

3. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi se davatelja usluga obvezalo da čuvaju u tajnosti činjenicu da je iskorišteno neko od ovlaštenja propisano ovim člankom, kao i sve informacije o tome.

4. Ovlaštenja i postupci navedeni u ovom članku bit će u skladu s člancima 14. i 15. ove Konvencije.

### Članak 21. – PRESRETANJE PODATAKA O SADRŽAJU

1. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi njena nadležna tijela, u odnosu na određena teška djela utvrđena unutarnjim pravom, bila ovlaštena u realnom vremenu:

a. prikupiti ili snimiti primjenom tehničkih sredstava na državnom području te stranke, te  
b. primorati davatelja usluga u okviru njegovih postojećih tehničkih mogućnosti da:

i. prikupi ili snimi primjenom tehničkih sredstava na državnom području te stranke i

ii. surađuje i pomogne nadležnim tijelima da prikupe i snime podatke o sadržaju u vezi s određenim komunikacijama na svojem državnom području prenesenima pomoću računalnog sustava.

2. Kada stranka zbog uspostavljenih načela svojega unutarnjeg pravnog sustava ne može usvojiti mjere navedene u točki (a) stavka 1., ona može umjesto toga usvojiti zakonske i druge mjere potrebne kako bi se osiguralo prikupljanje ili snimanje u realnom vremenu podataka o sadržaju podataka o navedenim komunikacijama na njenom državnom području kroz primjenu tehničkih sredstava na tom području.

3. Svaka stranka će usvojiti zakonske i druge mjere potrebne kako bi se davatelje usluga obvezalo da čuvaju u tajnosti činjenicu da je iskorišteno neko od ovlaštenja propisano ovim člankom, kao i sve informacije o tome.

4. Ovlaštenja i postupci navedeni u ovom članku bit će u skladu s člancima 14. i 15. ove Konvencije.

[Cijeli tekst Konvencije vidi ovdje](#)

# Zakonske smjernice

If your investigation ends up in a court of law, be prepared to provide evidence that the tools you used did their job without corrupting the evidence. That can be a tough sell if you try to prove it by yourself. An easier course would be to use commercially available forensic tools that have been accepted by courts. If in doubt, ask your local law enforcement contact which tools are accepted in local courts. If you use tools a judge has seen before, you are likely to avoid a lot of wasted time.

From:

<https://www.cis.hr/WikiIS/> - **wikiIS**

Permanent link:

[https://www.cis.hr/WikiIS/doku.php?id=zakoni\\_forenzika](https://www.cis.hr/WikiIS/doku.php?id=zakoni_forenzika)

Last update: **2015/01/21 13:37**

