



REPUBLIKA E SHQIPËRISË  
PROKURORIA PRANE GJYKATES SE SHKALLES SE PARE \_\_\_\_\_

Nr. \_\_\_\_\_ Prot. (Inicialet e emrit dhe mbiemrit)  
*Treguesi i urgjencës / Konfidencialitetit*

Tiranë më, \_\_\_\_ . \_\_\_\_ . 2016

**Lënda:** Kërkesë për ndihmë juridike drejtuar autoriteteve gjyqësore të \_\_\_\_\_  
lidhur me procedimin penal nr. \_\_\_\_\_ datë/viti

**MINISTRISË SË DREJTËSISË**

*Drejtorisë së Përgjithshme të Jetësimit të Prioriteteve,  
Marrëdhënieve Juridiksionale me Jashtë dhe Integritimit  
Drejtorisë së Marrëdhënieve Juridiksionale me Jashtë*

**TIRANË**

*Për dijeni:*

**PROKURORISË SË PËRGJITHSHME**

*Drejtorisë së Marrëdhënieve Juridiksionale me Jashtë*

**TIRANË**

*(Letërporosia do të shoqërohet nga kjo shkresë përcjellëse e cila do t'i drejtohet Ministrisë së Drejtësisë dhe për dijeni Prokurorisë së Përgjithshme si më poshtë:)*

Mbështetur në nenin 15 të Konventës së Këshillit të Evropës për Ndihmë të Ndërsjellë Juridike në Fushën Penale, nenin 509 të Kodit të Procedurës Penale dhe nenin 6 të Ligjit nr.10193, datë 03.12.2009 “Për Marrëdhëniet Juridiksionale me Autoritetet e Huaja në Çështjet Penale”, ju përcjellim bashkëlidhur, me qëllim transmetimin autoriteteve \_\_\_\_\_ të drejtësisë, kërkesën për ndihmë juridike në kuadër të **procedimit penal nr. \_\_\_\_\_, të vitit \_\_\_\_\_**, regjistruar për veprën penale të “\_\_\_\_\_”, parashikuar nga neni \_\_\_\_\_ i Kodit Penal.

*Duke ju falenderuar për bashkëpunimin,*

**DREJTUESI I PROKURORISË**

**EMRI MBIEMRI, FIRMA**



REPUBLIKA E SHQIPËRISË

PROKURORIA PRANË GJYKATËS SË SHKALLËS SË PARË \_\_\_\_\_

Tiranë më \_\_\_\_\_.2016

*Treguesi i urgjencës / Konfidencialitetit*

**KËRKESË PËR NDIHMË JURIDIKE**

**DREJTUAR AUTORITETIT GJYQËSOR KOMPETENT TË \_\_\_\_\_** (shëno Shtetin p.sh:  
Republikës së Italisë, dhe nëse dihet saktësisht qytetin përkatës)

Prokuroria e Rrethit Gjyqësor \_\_\_\_\_ u kërkon autoriteteve \_\_\_\_\_ të drejtësisë dhënien e ndihmës juridike në kuadër të,

procedimit penal nr. \_\_\_\_\_, datë \_\_\_\_\_  
për veprën penale të \_\_\_\_\_, parashikuar nga \_\_\_\_\_  
në ngarkim të \_\_\_\_\_,

*(Këtu të jepen gjithashtu të dhënat mbi subjektin (nëse ka) me të cilin lidhet objekti i letërporosisë si dhe të përcaktohet pozita e tij në procedim penal: i pandehur, dëshmitar, etj)*

Emri

Mbiemri

Aliase [nëse ka]

Data e lindjes [nëse nuk dihet mos e përfshini]

Vendi i lindjes [nëse nuk dihet mos e përfshini]

Shtetësia [nëse nuk dihet mos e përfshini]

Adresa [adresa e vendbanimit ose vendqëndrimit]

[Mund të plotësoni gjithashtu të dhëna të tjera që i konsideroni të arsyeshme, si psh numrin e pasaportës, përshkrimin fizik të subjektit, etj. Nëse është më shumë se një person, të dhënat e subjekteve të renditen në mënyrë kronologjike sipas përshkrimit tek përmbledhja e fakteve dhe sipas rëndësisë në lidhje me kërkesën]

**A. Përmbledhje e fakteve penale:**

*(Të bëhet një përmbledhje e shkurtër e fakteve që lidhen me procedimin penal përkatës duke renditur ato fakte për të cilat justifikohet dhe ndihma që u kërkohet autoriteteve të huaja, konkretisht,*

- *Përmbledhje e fakteve relevante që tregojnë kohës, vendin dhe mënyrën e kryerjes së veprës*
- *Përshkrimi i qartë i lidhjeve ndërmjet veprës dhe personit dhe ndërmjet veprës dhe provave/masave/ aseteve kriminale të kërkuara në shtetin e kërkuar.*

*Ku është e aplikueshme*

- *Dëme të shkaktuara nga vepra*
- *Informacion mbi viktimat*
- *Ku është e nevojshme, dispozitat mbi kalimin e afatit*
- *Çdo informacion tjetër shtesë që mund të ndihmoj autoritetin kërkues në kryerjen e kërkesës)*

***B. Teksti i dispozitave ligjore të zbatuara (këtu mund të shënohet teksti i nenit apo neneve përkatëse)***

### ***C. Baza ligjore dhe ndihma e kërkuar***

*Mbështetur në (Do shënohet konventa shumëpalëshe apo marrëveshja dy-palëshe përkatëse në fuqi e cila mund të jetë një ose më shumë) Konventën \_\_\_\_\_ për \_\_\_\_/Marrëveshjen ndërmjet Republikës së Shqipërisë, kërkojmë nga ana e autoriteteve gjyqësore kompetente të \_\_\_\_\_, kryerjen e veprimeve të mëposhtme proceduriale:*

*(rendisni me saktësi veprimet e kërkuara, për lehtësi konsultohuni me veprimet e përshkruara në Anex 2)*

*{Më poshtë për lehtësi reference në Anex 1 po rendisim Konventat shumëpalëshe dhe disa nga Marrëveshjet Dy-palëshe të ratifikuara nga Republika e Shqipërisë në fushën e asistencës së ndërsjellë juridike në çështjet penale}*

***D. Sa më poshtë (urgjenca dhe procedura e posaçme) janë opsionale duke u vlerësuar rast pas rasti:***

***Urgjenca*** *(në rast se veprimet e kërkuara paraqesin urgjencë t'u theksohet kjo gjë autoriteteve të huaja ose të përcaktohet një afat i arsyeshëm për realizimin e këtyre veprimeve, së bashku me arsyet e urgjencës apo afatit).*

***Procedura e Posaçme*** *(në rast se nga ana juaj ka kërkesa specifike për mënyrën e ekzekutimit të letërporosisë, psh marrja në pyetje e personit të bëhet para gjykatës së huaj, etj, të përcaktohet shprehimisht procedura që duhet ndjekur nga autoriteti i huaj. Kjo është e nevojshme pasi duhet pasur gjithmonë parasysh që provat e marra me letërporosi të pranohen nga gjykata. Autoritetit të huaj mund t'i kërkohet gjithashtu edhe përcjellja e një kopjeje të materialeve në ekzekutim të letërporosisë në mënyrë të drejtëpërdrejtë, duke përcaktuar se ku do të dërgohen (në*

*Prokurorinë tuaj apo në Prokurorinë e Përgjithshme) ndërkohë që aktet origjinale t'i transmetohen ndërkohë autoritetit qendror, Ministrisë së Drejtësisë.*

Deklarojmë se, të dhënat/informacionet e marra në ekzekutim të kësaj letërporosie do të përdoren nga autoritetet gjyqësore shqiptare vetëm për nevoja të këtij procedimi penal në përputhje me legjisllacionin kombëtar.

***E. Të dhënat e kontaktit***

Për çdo informacion të mëtejshëm lidhur me këtë kërkesë, lutemi të *(mund të vendosni të dhënat e kontaktit që i shihni të arsyeshme)* kontaktoni me:

**Drejtorinë e Marrëdhënieve Juridiksionale me Jashtë në Prokurorinë e Përgjithshme,**

në: tel/fax: 00355 42 235232

e-mail: [foreign.department@pp.gov.al](mailto:foreign.department@pp.gov.al)

**Prokurorin e çështjes**

Emër Mbiemër:

Adresa:

Telefoni:

E-mail:

*Duke ju falenderuar paraprakisht për bashkëpunimin tuaj,*

**PROKURORI I ÇËSHTJES**

**(EMRI MBIEMRI, firma)**

## ANEX 1

### *Konventat Shumëpalëshe*

- Konventa e Këshillit të Evropës për Ndhmën e Ndërsjellë Juridike në Fushën Penale dhe Protokollin e saj Shtesë (ratifikuar me Ligjin nr. 8498, datë 10.6.1999)
- Protokollin e Dytë shtesë të Konventës së Këshillit të Evropës për Ndhmën e Ndërsjellë Juridike në Fushën Penale (ratifikuar me Ligjin nr. 8883, datë 18.4.2002)
- Konventa e Kombeve të Bashkuara kundër Krimit të Organizuar Ndërkombëtar dhe dy Protokollin e saj Shtesë (ratifikuar me Ligjin nr. 8920, datë 11.07.2002).
- Konventa e Kombeve të Bashkuara kundër trafikut të paligjshëm të drogave narkotike dhe të lëndëve psikotrope (ratifikuar me Ligjin nr. 8722, datë 26.12.2000)
- Konventa Penale për Korrupsionin (ratifikuar me Ligjin nr. 8778, datë 26.4.2001)
- Konventa për Krimin në Fushën e Kibernetikës (ratifikuar me Ligjin nr. 8888, datë 25.4.2002)
- Protokollin e shtesë të Konventës për krimin kibernetik, për penalizimin e akteve me natyrë raciste dhe ksenofobe të kryera nëpërmjet sistemeve kompjuterike (ratifikuar me Ligjin nr. 9262, datë 29.7.2004)
- Konventa Europiane për Pastrimin, Depistimin, Kapjen dhe Konfiskimin e Produkteve të Krimit (ratifikuar me Ligjin nr. 8646, datë 20.7.2000)

### *Marrëveshjet Dypalëshe*

- Marrëveshja ndërmjet Republikës së Shqipërisë dhe Republikës së Italisë, si shtesë e Konventës Europiane për Ekstradimin, të 13 dhjetorit 1957 dhe e Konventës Europiane për Ndhmë Juridike për Çështjet Penale, të 20 prillit 1959 (ratifikuar me Ligjin nr. 9871, datë 11.2.2008)
- Konventa për ndihmën e ndërsjellë gjyqësore në fushat civile, tregtare dhe penale ndërmjet Republikës së Shqipërisë dhe Republikës së Turqisë (ratifikuar me Ligjin nr. 8036, datë 22.11.1995)
- Marrëveshje ndërmjet qeverisë së Republikës së Shqipërisë dhe qeverisë maqedonase për ndihmën juridike në fushën civile dhe penale (ratifikuar me Ligjin nr. 8304, datë 12.3.1998)
- Konventa ndërmjet Republikës së Shqipërisë dhe Greqisë për ndihmën gjyqësore në çështjet civile dhe penale (ratifikuar me Ligjin nr. 7760, datë 14.10.1993)
- Marrëveshjen Dypalëshe ndërmjet Këshillit të Ministrave të Republikës së Shqipërisë dhe Qeverisë së Republikës së Kosovës “*Për ndihmë të ndërsjellë juridike në çështjet penale*”,

## ANEX 2

### ***i. LLOJET E VEPRIMEVE PROCEDURIALE***

#### **a. Seancë dëgjimi/marrja në pyetje e dëshmitarëve, ekspertëve, të dyshuarve, personave të akuzuar dhe personave të tjerë: modalitete të veçanta**

##### **a1. Marrja në pyetje nga autoriteti i kërkuar (shtetit të cilit i dërgohet letërporosia)**

- Të dhënat e autoritetit kompetent i cili duhet të kryejë marrjen në pyetje
- Të dhënat mbi cilësinë e personit që do të merret në pyetje
- Informacion mbi të drejtat dhe detyrimet e subjektit që do të merret pyetje (si për shembull, e drejta për t'u ndihmuar nga një avokat/përkthyes etj.)
- Lista e pyetjeve që do t'i drejtohet subjektit

##### *Kur është e zbatueshme*

- Të dhëna nëse personi që do të dëgjohet kërkon mbrojtje (duke përfshirë detaje mbi marrëveshjet e mundshme ekzistuese ndërmjet të dy palëve mbi këtë çështje)

##### **a2. Marrja në pyetje nëpërmjet video-konferencës ose lidhjeve telefonike**

- Emri i autoritetit gjyqësor që realizon marrjen në pyetje (nëse dihet)
- Detaje në lidhje me aspektet teknike (informacion teknik mbi mjetet në dispozicion, propozimet në lidhje me pagesën e kostove, të dhënat e kontaktit për personin e kontaktit teknik IT, etj.)
- Të drejtat dhe detyrimet që do t'i njoftohen personit që do të merret në pyetje
- Data/koha e propozuar

##### *Ku është e aplikueshme*

- Të përcaktohet nëse është e nevojshme prezenca e një përkthyesi
- Të përcaktohet nëse duhet të merren masa për mbrojtjen e personit që do të merret në pyetje
- Lista e pyetjeve që do t'i drejtohet personit

### **b. Marrja e provave**

#### **b1. Veprimet e përgjithshme**

- Identifikimi i sendeve/objekteve/dokumenteve/informacioneve të kërkuara

#### **Kontrolle dhe sekuestrime**

- Lloji i kontrollit: kontrolli i personit/banesës/vendeve të tjera;

- Për aq sa është e mundur saktësoni të dhënat identifikuese të personit, ose vendet që do të kontrollohen
- Të përcaktohen saktë dokumentet, regjistrat apo të dhënat e tjera që do të sekuestrohen

*Kur është e zbatueshme*

- Jepni detaje mbi lidhjen ndërmjet personit, procedimit të huaj dhe masave të kërkuara p.sh. vendi që do të kontrollohet
- Kopje e urdhrat/vendimit të lëshuar nga autoriteti kërkuar.

## **b2. Masat e veçanta:**

### **• b2.1. Të dhënat elektronike**

#### **➤ Ruajtja e të dhënave**

- Të jepet informacioni i nevojshëm për të identifikuar të dhënat specifike për tu ruajtur duke përfshirë vendndodhjen e tyre (Personi/ Shoqëria/Kompania e të dhënave kompjuterike të ruajtura, vendndodhja e sistemit kompjuterik)
- Të jepen arsytet në bazë të të cilave mendohet se ka rrezik për humbjen apo modifikimin e të dhënave
- Konfirmimi se do të paraqitet më pas një kërkesë për ndihmë juridike me qëllim marrjen e të dhënave të ruajtura.

#### **➤ Kontrolli apo aksesimi i ngjashëm me të, sekuestrimi/ruajtja/dhënia e informacionit**

- Qëllimi specifik
- Të jepet informacioni i nevojshëm për të identifikuar të dhënat që kërkohen të sekuestrohen, ruhen apo jepen, duke përfshirë, nëse dihet, vendndodhjen fizike e tyre dhe personin që i ka në kontroll të dhënat
- Për aq sa është e mundur, identifikim i saktë i personit/ambienteve që do të kontrollohen duke dhënë ndërkohë detaje mbi lidhjet ndërmjet personit, të dhënave dhe vendit që do të kontrollohet
- Pika e kontaktit

*Ku është e aplikueshme*

- Informacion mbi një kërkesë të mëparshme për ruajtjen e të dhënave

*Për informacione më të detajuara mbi letërporositë në fushën e krimit kibernetik shihni ANEX 3*

### **• b2.2. Sekuestrimi dhe/ose konfiskimi i aseteve kriminale**

- Arsytet pse mendohet se asetet ndodhen në shtetin e kërkuar
- Të tregohet procedura që kërkohet të ndiqet nga autoritetet shqiptare
- Bashkëlidhur: kopje e vendimit të sekuestrimit/konfiskimit;
- Informacion në lidhje me llogaritë bankare në shtetin e kërkuar

## **c. Marrjen e informacionit nga institucionet financiare**

- Detajet e institucionit financiar (emri i bankës ose institucionit financiar, adresa e degës, ku mbahet llogaria)
- Numri i llogarisë
- Tregues i periudhës për të cilën kërkohet informacioni
- Arsyet për të besuar se llogaria ndodhet në shtetin e kërkuar

#### **d. Marrja e të dhënave telefonike / IP**

##### **d1. Informacioni në lidhje me të dhënat telefonike**

- Tregues i numrit të telefonit
- Informacioni në lidhje me zotëruesin e numrit të telefonit
- Tregues i periudhës për të cilën të dhënat e telefonit janë të nevojshme

##### **d2. Informacioni në lidhje me të dhënat e IP**

- Tregues i adresës IP, ku kërkohet identifikimi i përdoruesit (kur Adresa e IP është e njohur), i vulës së kohës (dita dhe koha e përdorimit) dhe të emrit të ISP
- Të dhëna për emrin dhe adresën e të dyshuarit (kur ai/ajo është i njohur, por Adresa e IP së përdoruesit konkret nuk dihet) dhe, nëse dihet, datën dhe kohën e përdorimit dhe emrin e ISP

#### **e. Kryerja e Ekspertizës**

- Informacion mbi ekspertizën kërkuar

*Ku është e aplikueshme*

- Lista e pyetjeve për t'u përgjigjur nga eksperti

#### **f. Përgjimi i komunikimeve**

- Çdo informacion i rëndësishëm mbi statusin e personit dhe mbi lidhjen ndërmjet nevojës për përgjim dhe hetimit në vazhdim në përputhje me kërkesat ligjore të shtetit kërkuar

*Ku është e aplikueshme*

- Informacion mbi afatin kohor

#### **ii. MODALITETET PËR TRANSMETIMIN E PROVAVE**

- Tregoni nëse origjinalet janë të nevojshme
- Mjetet e preferuara të transmetimit që do të përdoren nga shteti i kërkuar (korrier, oficer ndërlidhës, përfaqësues diplomatik, etj.)
- Kopje paraprake e akteve të kërkuara

**A. Dërgimi i dokumenteve gjyqësore (njoftimi i urdhrave/vendimeve të autoriteteve gjyqësore/dokumenteve të tjera; njoftimi i aktit të thirrjes ndaj personit nën hetim/ të pandehurit/dëshmitarit/ekspertit/të dënuarit apo palëve të tjera në proces):**



***i. Informacion i përbashkët për të gjitha kërkesat e shërbimit***

- Lloji i shërbimit të nevojshëm
- Specifikimi i dokumenteve për t'u paraqitur

*Ku është e aplikueshme:*

- *Informacion mbi mbrojtjen e dëshmitarëve*
- *Kërkesat për konfirmimin e njoftimit*
- *Kërkesat nëse njoftimi nuk realizohet*
- *Miratimi i supozimit të shpenzimeve*

***ii. Informacion për përmbledhjet që duhet të paraqiten***

- Data e paraqitjes
- Koha dhe vendi i seancës së dëgjimit

*Ku është e aplikueshme:*

- *Data alternative e paraqitjes, koha dhe vendi i seancës së dëgjimit*
- *Shtesat e pagueshme të përafërta dhe shpenzimet e pakthyeshme të qëndrimit dhe të udhëtimit*
- *Kartë Visa ose kërkesat e tjera të hyrjes*

**B. Ekstraktet nga regjistrat gjyqësor**

- Identifikimi i personit për të cilin kërkohet gjendja gjyqësore/rekordet kriminale

### **ANEX 3**

## **UDHËZUES HETIMOR PËR SIGURIMIN E PROVAVE ELEKTRONIKE NGA SHTETET E BASHKUARA**

### *Parathënie dhe falenderime*

Qëllimi i këtij udhëzuesi është t'u sigurojë hetuesve dhe prokurorëve të huaj një mjet për të kuptuar ligjet për mbledhjen dhe dhënien e provave elektronike brenda SHBA-së. Ky udhëzues është hartuar për t'u përdorur si ndihmë, jo si autoritet. Për rrjedhojë, analiza dhe përfundimet e përfshira këtu pasqyrojnë mendimin aktual për çështje të vështira dhe dinamike të ligjit; si të tilla, ato nuk mund të përfaqësojnë pozicionin e tanishëm zyrtar të Departamentit të Drejtësisë apo të ndonjë organi tjetër.<sup>1</sup>

Ky udhëzues është produkt i Divizionit të Krimeve të Departamentit të Drejtësisë së Shteteve të Bashkuara dhe është një përpjekje e përbashkët e Seksionit për Krimin Kompjuterik dhe Pronësinë Intelektuale (KKPI) dhe Zyrës së Marrëdhënieve Ndërkombëtare (ZMN).

---

<sup>1</sup> Ky udhëzues nuk ka efekt rregullator, nuk siguron të drejta apo zgjidhje dhe nuk ka forcën e ligjit apo të një direktive të Departamentit të Drejtësisë të SHBA.

## 1. Tablo e provave elektronike në Shtetet e Bashkuara

Ka dy kategori bazë të provave elektronike të cilat kërkohen vazhdimisht nga punonjësit e zbatimit të ligjit: (1) **informacioni i ruajtur** (psh. informacion për abonentin, emaile apo mesazhe zanore të dërguara më parë dhe të dhënat se kur një individ ka përdorur llogarinë e tij) dhe (2) **komunikime në kohë reale** (psh. informacioni i mbledhur ndërkohë që komunikimi është duke u kryer). Kuadri ligjor i SHBA-së i klasifikon të dhënat mbi bazën e nivelit të fshehtësisë që ato përbëjnë përsa i takon mbajtësit të një llogarie të caktuar. Përgjithësisht, sa më thellë të preket fshehtësia e individit, aq më e madhe është barra ligjore që ka shteti për t'i siguruar këto të dhëna. Sigurimi i informacionit bazë për abonentin (emri i mbajtësit të llogarisë dhe adresa), për shembull, e prekin më pak fshehtësinë e tij sesa sigurimi i përmbajtjes së një mesazhi të padërguar dhe për rrjedhojë, barra ligjore që duhet plotësuar për të siguruar informacionin e abonentit është më pak e mundimshme sesa ajo që nevojitet për të siguruar përmbajtjen e mesazheve të padërguara. Në të njëjtën mënyrë, të sigurosh informacion të ruajtur konsiderohet si shkelje më e vogël e fshehtësisë personale sesa gjurmimi i komunikimit në kohë reale. Pra, kur kërkohen prova elektronike, punonjësit e policisë dhe prokurorët duhet të mbajnë parasysh klasifikimet e ndryshme që përcaktohen në Seksionin 3 dhe të sigurojnë informacionin e nevojshëm, në varësi të të dhënave që kërkojnë.

**KËSHILLË PRAKTIKE** – Kërkoni vetëm atë që ju nevojitet me të vërtetë; sa më shumë të kërkoni, aq më tepër kohë do të duhet dhe aq më i lartë do të jetë standardi i provës që mund të kërkojë gjykata amerikane për të autorizuar marjen e saj. Nëse më pas zbuloni se ju duhet më shumë informacion, mund të bëni një kërkesë tjetër.

## 2. Situatat e urgjencës

Në situatat e urgjencës, legjislativi i SHBA-së i lejon punonjësit e policisë të përfshihen në disa veprimtari hetimore pa siguruar miratim paraprak nga gjykata. Kjo zbatohet në situatat e urgjencës në SHBA ose jashtë vendit dhe informacioni shpesh mund të sigurohet pa kërkesë zyrtare. Shembuj të këtyre urgjencave mund të përfshijnë një rast rrëmbimi kur rrëmbyesi komunikon me familjen e të rrëmbyerit duke përdorur një llogari emaili; një rast terrorizmi kur terroristi përdor një llogari emaili për të planifikuar një sulm të afërt; ose një sulm që shkakton ndërprerjen e shërbimit, ndaj serverave të brendshëm të një spitali, gjë që bën të pamundur ofrimin e kujdesit ndaj pacientëve.

Në situatat urgjente, autoritetet e zbatimit të ligjit në SHBA ose në vende të tjera mund të kërkojnë dhënien e informacionit nga një ofrues i shërbimit të internetit (në vazhdim “OSHI”)

pa miratimin paraprak të gjykatës (Shënim: Kjo është një kërkesë për rast të “jashtëzakonshëm” dhe mund të përdoret vetëm në raste urgjencash reale). OSHI mund të japë vullnetarisht secilën prej tre llojeve të të dhënave të cilat lidhen me informacionin e ruajtur që diskutohet më poshtë (psh. informacion për abonentin, informacion për një transaksion dhe për përmbajtjen). Gjithësesi, kini parasysh se autoriteti për të dhënë informacion në rast urgjence lejon vetëm që përmbajtja e komunikimeve t’i bëhet e ditur një agjencie të zbatimit të ligjit në SHBA. Për ta përdorur këtë procedurë urgjence, ligji parashikon që OSHI duhet të bindet se:

- i) Ka një urgjencë që përfshin një “rrezik të çastit për jetën ose dëmtimin e rëndë fizik të një personi” (mundësitë hipotetike të rrezikut nuk do ta plotësojnë këtë kusht); dhe
- ii) Ky rrezik kërkon dhënien pa vonesë të informacionit.

Megjithatë kini parasysh se ofruesit e shërbimit të internetit nuk janë të detyruar ta japin informacionin. Nëse OSHI refuzon të japë të dhënat e kërkuara “vullnetarisht”, mbetet ende mundësia e përdorimit të procesit ligjor për të kërkuar marrjen e të dhënave.

### 3. Çështje paraprake

#### *a. Mbajtja/ruajtja e të dhënave*

Në situatat jo urgjente, hapi i parë në çdo hetim që ka të bëjë me provat elektronike, është të ruhen provat para se ato të fshihen në mënyrë të pakthyeshme. Koha ka rëndësi thelbësore. Në momentin që fshihen, këto mesazhe përgjithësisht nuk mund të rikthehen më nga një OSHI. Pjesa më e madhe e OSHI-ve fshijnë në mënyrë të përhershme dhe periodike të dhënat e transaksioneve nga serverat e tyre; nuk ka asnjë ligj në SHBA që të parashikojë mirëmbajtjen apo shkatërrimin e këtyre të dhënave. OSHI-t shpesh i fshijnë këto të dhëna nga 21 ditë deri në 6 muaj pasi është zhvilluar komunikimi. Kërkesat për komunikimet elektronike që kanë ndodhur para gjashtë muajsh, rrallë marrin përgjigje pozitive.

Kjo është një procedurë e thjeshtë. Disa OSHI pranojnë kërkesa për ruajtjen e informacionit drejtpërdrejt nga organe të huaja të zbatimit të ligjit. Përderisa kjo është një praktikë vullnetare e OSHI-ve dhe procedurat dhe praktikat në lidhje me kërkesat për ruajtje nga jashtë variojnë; shtetet e tjera nxiten të verifikojnë drejtpërdrejt me OSHI-n përkatës. Në raste të tjera, kërkesën mund ta transmetojë përfaqësuesi i vendit tuaj për Rrjetin e Krimin të Teknologjisë së Lartë 24 orë çdo ditë të javës (që përkrahë më poshtë). Përgatituni të jepni faktet bazë të hetimit dhe llogarinë konkrete/adresën e IP-së/façen elektronike që duhet të ruhet,

si edhe datën dhe orën korresponduese (ku përfshihet edhe zonat orare që përdorura). Nëse ju nevojiten udhëzime shtesë ose nëse vendi juaj nuk është anëtar i rrjetit 24 orë, mund të kontaktoni një sërë burimesh, duke përfshirë të dërguarin për çështjet e zbatimit të ligjit pranë Ambasadës së Shteteve të Bashkuara në vendin tuaj ose të Departamentit të Drejtësisë të SHBA (KKPI ose ZMN).

Shumica e OSHI-ve i ruajnë të dhënat për 90 ditë pasi marrin kërkesën për ruajtje dhe ajo mund të rinovohet edhe për 90 ditë të tjera me një kërkesë me shkrim. Pavarësisht metodës së zgjedhur, menjëherë pasi është kërkuar ruajtja, vendi që ka bërë kërkesën duhet të fillojë ndjekjen e njëres prej metodave për marrjen e informacionit (për shembull, nëpërmjet shkëmbimit jozyrtar të informacionit ndërmjet organeve të zbatimit të ligjit si pjesë e një hetimi të përbashkët ose dorëzimit të një kërkesë zyrtare, ku përfshihet edhe një kërkesë në përputhje me Marrëveshjen për Ndihmë Ligjore të Ndërsjellë (MNLN)).

i. Rrjeti i teknologjisë së lartë 24 orë (Personat e kontaktit)

Një grup prej më shumë se 50 shtete kanë ngritur njësi hetimore për teknologjinë e lartë të cilat merren 24 orë në ditë me hetimin e krimeve që lidhen me kompjuterat. Nëse vendi juaj është anëtar i këtij rrjeti, përfaqësuesi i vendit tuaj mund të bashkëpunojë direkt me përfaqësuesit amerikanë për të ruajtur provat elektronike sa më shpejt që është e mundur.

*b. Aspekte të tjera për t'u marrë parasysh*

i. Njoftim për abonentët

Kur dorëzohet një kërkesë për ruajtjen e informacionit, ka një mundësi që zotëruesi i llogarisë të marrë vesh për hetimin, pasi strukturat teknike të ofruesit janë krijuar si pjesë të serverave të tyre ose për shkak se vetë ofruesi e bën një njoftim të tillë. Megjithatë përgjithësisht, klientët e OSHI-ve më të mëdha dhe më të njohura nuk informohen për ekzekutimin e kërkesës për ruajtje.

## ii. A është i besueshëm OSHI?

Kur drejtoni kërkesa për ruajtje apo produkte tek OSHI-t, mbani mend se jo të gjithë ofruesit janë të besueshëm. Domethënës është fakti që nuk ka kritere për licensimin e OSHI-ve në SHBA dhe ka shumë pak rregulla që normojnë industrinë e këtyre ofruesve. Për shembull, ka raste kur një OSHI drejtohet nga një organizatë kriminale, pra, kur dërgohet një kërkesë e tillë, ka mjaft të ngjarë që personi që është nën hetim të njoftohet menjëherë. Për pasojë, para se të dorëzoni një kërkesë të tillë tek një OSHI e panjohur, shqyrtoni mundësinë që të kontaktoni me autoritetet e SHBA-së për t'u siguruar se ofruesi është i njohur dhe i besueshëm.

## iii. Filiale të huaja të OSHI-ve në SHBA

Në disa raste, OSHI me qendër në SHBA kanë krijuar filiale në vende të tjera. Në këto raste, filiali i huaj i një OSHI amerikan mund të ofrojë drejtpërdrejt një lloj ndihme që përshkruhet në këtë udhëzues për autoritetet e huaja të zbatimit të ligjit, pa pasur nevojë për një kërkesë zyrtare drejtuar SHBA-së. Meqënëse OSHI-t operojnë sipas strukturave të ndryshme organizative, ligjore dhe nënligjore dhe mqs praktikant mund të ndryshojnë me kalimin e kohës, filialet e huaja të OSHI-t duhet të konsultohen drejtpërdrejt për këtë pikë.

### *c. Procesi në SHBA për shqyrtimin dhe ekzekutimin e kërkesave ndërkombëtare*

Kur merret një kërkesë për ndihmë nga një vend tjetër, një jurist i ZMN-së e shqyrton kërkesën për të përcaktuar nëse ajo paraqet informacionin e mjaftueshëm, siç parashikohet në marrëveshjet dhe ligjet përkatëse dhe nëse po, cila është mënyra më e mirë për ta ekzekutuar kërkesën. Nëse kërkesa gjykohet të jetë e pamjaftueshme pjesërisht apo tërësisht, ZMN-ja mund të kërkojë informacion shtesë nga vendi që e ka drejtuar kërkesën para se të merret një vendim përfundimtar për ekzekutimin e saj.

### *d. Për t'u pasur parasysh në rastet e terrorizmit*

Kur merren prova elektronike në çështjet që lidhen me terrorizmin, duhet të merren në konsideratë disa faktorë të veçantë. Në këto raste, është e detyrueshme të bashkërendohen veprimet nga ZMN-ja dhe përfaqëuesit e SHBA-së për çështjet e zbatimit të ligjit në Ambasadën e SHBA-së në vendin tuaj, para se të dorëzoni kërkesën; ky konsultim do t'ju ndihmojë për një trajtim të shpejtë dhe të duhur të kërkesës suaj.

#### 4. Informacioni i ruajtur – Tre lloje

Ka tre lloje informacioni të ruajtur që mund të sigurohet nga OSHI-t dhe që është i dobishëm për hetimin:

*a. **Informacioni për abonentin** – Niveli më i ulët i procesit*

#### **Çfarë është?**

Informacioni për abonentin është informacion që përshkruan se kush është personi (psh. emri dhe adresa e abonentit) dhe përfshin informacion bazë për përdorimin që një person i bën shërbimit online (OSHI) në një datë dhe orë të caktuar (për shembull, orët kur ka përdorur llogarinë, për sa kohë e ka përdorur abonentin një shërbim të caktuar, etj.).

#### **Standardi ligjor**

Për të siguruar informacion për abonentin, duhet të vërtetoni se provat që kërkohen janë të rëndësishme dhe në lidhje me hetimin penal. Nuk mjafton të tregosh se personi i akuzuar ka një llogari email; llogaria duhet të ketë një lloj lidhjeje me veprën që po hetohet. Ky është standardi më i ulët ligjor që kërkohet në një proces hetimor.

#### **Shembuj kur informacioni për abonentin mund të jetë i rëndësishëm**

Rasti hipotetik nr. 1 (shfrytëzim të miturish)

Viktoria, 12 vjeçe, ka marrë një email që ka bashkëngjitur fotografi të fëmijëve gjatë kryerjes së akteve seksuale nga një i rritur i dyshuar, që përdor adresën [Joe@us-ISP.com](mailto:Joe@us-ISP.com). Në këtë email, Xho sugjeron që ata të takohen në një vend të

caktuar. Punonjësi i policisë dëshiron të dijë se në emër të kujt është regjistruar kjo llogari emaili (dhe për rrjedhojë nuk ka nevojë të njohë përmbajtjen e llogarisë së emailit).

#### Rasti hipotetik nr. 2 (kërcënim për marrje pasurie)

Korporata ABC ka marrë një email ku dërguesi kërcënon se do të nxjerrë informacion të fshehtë për klientët e korporatës nëse nuk merr 100,000 dollarë. Dërguesi jep një link tek një faqe elektronike që mbrohet me fjalëkalim, e cila përmban informacion të fshehtë për klientët e ABC-së si provë, si edhe fjalëkalimin që i nevojitet korporatës për të parë informacionin dhe për të verifikuar kërcënimin. Hetuesi dëshiron të dijë se kush e zotëron këtë llogari emaili, kush e zotëron apo kujt i është caktuar adresa e IP-së që ka përdorur dërguesi për të hyrë tek llogaria e emailit dhe kush është regjistruar në këtë faqe elektronike.

#### Rasti hipotetik nr. 3 (vjedhje e informacionit elektronik)

Gjyshja merr një email që e informon se duhet ta përditësojë informacionin e llogarisë online tek [www.onlinebank.com](http://www.onlinebank.com) ku duhet të japë informacionin e saj personal. Tre ditë pasi e bën një gjë të tillë, në llogarinë e saj nuk kanë mbetur më pará. Gjyshja ia jep emailin fillestar që ka marrë një hetuesi i cili zbulon se linku nuk të çon në faqen zyrtare të bankës, por tek një faqe elektronike e një pale të tretë. Hetuesi ka nevojë të dijë se kush e ka krijuar këtë faqe elektronike, në ç'mënyrë është bërë pagesa për krijimin e saj, sa kohë ka hapur dhe ku është hapur.

### **Llojet e informacionit të disponueshëm për abonentin**

Më poshtë gjeni llojin e informacionit për abonentin që duhet të kërkoni (Shënim: kur kërkoni informacion, ju lutemi jepni një adresë të caktuar emaili [psh. [Joe@us-ISP.com](mailto:Joe@us-ISP.com)] ose një adresë IP-je [psh. adresa e IP-së 120.128.4.30] ose URL-në e një faqeje elektronike [psh. <http://www.onlinebank.com>] si edhe datën, orën dhe zonën orare):

1. Llogaria ose emri që përdor abonentit;
2. Emri i abonentit dhe adresa e rrugës;
3. Numri ose numrat e telefonit të abonentit;
4. Adresa e emailit të abonentit;



5. Adresa e Protokollit të Internetit (IP) që është përdorur nga abonenti për të regjistruar llogarinë ose për të filluar një shërbim tjetër;
6. Të gjitha adresat IP të përdorura nga abonenti për të hyrë në llogarinë e tij;
7. Orët, datat dhe kohëzgjatjet e këtyre sesioneve, si dhe
8. Çdo informacion tjetër që lidhet me identitetin e abonentit, duke përfshirë, por jo vetëm: informacionin për pagesën (ku përfshihen lloji dhe numri i kartave të kreditit, numri i identifikimit të studentit ose ndonjë informacion tjetër identifikues).

**KËSHILLË PRAKTIKE** – Për shkak se adresat e IP-ve ndryshojnë shpesh, është e rëndësishme të përfshini kohën e saktë – deri me sekonda, nëse është e mundur – si edhe zonën orare (psh. “GMT”) kur kërkon informacion për adresën e IP-së.

**KËSHILLË PRAKTIKE** – Bëni kujdes të shpjegoni se si lidhen afatet kohore të të dhënave që kërkohen (psh. data/ora e fillimit dhe përfundimit) me hetimin. Edhe pse për të siguruar informacion për abonentin duhet plotësuar standardi më të ulët ligjor, drejtuesit e organeve të zbatimit të ligjit gjithësesi duhet të justifikojnë se si provat e kërkuara lidhen me hetimin.

b. **Informacion për transaksionet** – *Niveli i mesëm i procesit*

### **Çfarë është informacioni për transaksionet?**

Të dhënat për transaksionet përfshijnë të dhëna që identifikojnë se më kë ka komunikuar një abonent, se cilat faqe elektronike ka vizituar ai/ajo dhe informacion të ngjashëm për veprimtarinë në internet të një përdoruesi.

### **Standardi ligjor**

Për të siguruar pjesën më të madhe të informacioneve që lidhen me transaksionet, duhet të jepni fakte specifike që përcaktojnë se si të dhënat dhe informacioni tjetër që kërkohet lidhen dhe janë pjesë përbërëse e hetimit. Kjo ndodh pasi ligji në Shtetet e Bashkuara parashikon që

prokurorët t'i paraqesin gjykatës një përmbledhje faktike të hetimit dhe se si të dhënat e kërkuara do ta ndihmojnë hetimin. Ky është një standard mesatar, më i lartë se ai bazë, por jo aq sa standardi ligjor i “shkakut të mundshëm,” siç parashikohet më poshtë në pjesën (c).

### **Shembuj ku informacioni për transaksionet mund të jetë i dobishëm ose i rëndësishëm**

Rasti hipotetik nr. 1 (shfrytëzim i të miturve)

Në rastin kur 12-vjeçares Viktoria iu kërkua të udhëtonte për të takuar “Xhonë,” hetuesi dëshiron të identifikojë edhe të mitur të tjerë që mund të jenë viktimizuar. Hetuesi kërkon adresën e emailit të përdorur për të komunikuar me llogarinë e emailit të “Xhosë”.

Rasti hipotetik nr. 2 (kërcënim për marrje pasurie)

Në rastin kur Korporata ABC mori emailin kërcënues, hetuesi dëshiron të dijë nëse dërguesi i emailit ka edhe bashkëpunëtorë të tjerë. Hetuesi tani kërkon një adresë emaili nga e cila janë dërguar apo janë marrë emaile.

Rasti hipotetik nr. 3 (vjedhje e informacionit elektronik)

Në rastin kur llogaria bankare e gjyshes ishte vjedhur nga një pirat elektronik, hetuesi dëshiron të dijë nëse ka edhe viktimat të tjera të mundshme që kanë marrë emaile të tilla mashtruese. Hetuesi tani kërkon edhe adresat e tjera emaili tek të cilat janë dërguar emaile të tilla.

### **Llojet e informacionit të disponueshëm për transaksionet**

Kur kërkonte informacion për transaksionet dhe jepni një adresë specifike emaili ose URL-në e një faqeje elektronike, ky është informacioni që duhet të kërkonte:

Për llogari emaili ose faqeje elektronike:

- Informacion lidhës me sistemet e tjera me të cilat përdoruesi është lidhur nga llogaria e tij e emailit (ose nga llogaria e faqes elektronike) ku përfshihen:
  - a. Destinacioni ose origjina e lidhjes;
  - b. Data dhe ora e lidhjes;
  - c. Data dhe ora e shkëputjes së lidhjes;
  - d. Metoda e lidhjes me sistemin (psh. telnet, ftp, http);
  - e. Vëllimi i transferimit të të dhënave (psh. bait (bytes) dhe
  - f. Çdo informacion tjetër për rrugët lidhëse (route);
- Origjinën apo destinacionin e ndonjë mesazhi tjetër elektronik që është dërguar apo marrë nga kjo llogari (që njihet si koka e emailit ose fushat “To” (Për) dhe “From” (Nga), si dhe datën, orën dhe gjatësinë e mesazhit;
- Informacion në lidhje me çdo imazh apo dokument tjetër që është ngarkuar në këtë llogari (ose faqe elektronike), ku përfshihet data dhe ora e ngarkimit, si dhe madhësia e skedës (file), por jo përmbajtja e saj;
- Emri dhe detaje të tjera identifikuese të individit që ka hapur një imazh/skedë/faqe elektronike të caktuar në një periudhë të caktuar kohe dhe në një datë të caktuar.

*c.      **Përmbajtja** – Niveli më i lartë i procesit*

**Çfarë është?**

Përmbajtja është informacioni i dërguar në një email nga dërguesi tek marrësi, që mund të përfshijë mesazhe të shkruara, fotografi apo imazhe ose materiale të bashkëngjitura.

**Standardi ligjor**

Në pjesën më të madhe të rasteve, për të siguruar përmbajtjen duhet që informacioni në kërkesën zyrtare të plotësojë dy standarde ligjore: (1) “shkakun e mundshëm” dhe (2) të vërtetojë se faktet që mbështesin kërkesën janë aktuale.

“**Shkaku i mundshëm**”: kërkesa duhet të paraqesë fakte specifike që mbështesin dyshimin se provat (përmbajtja) e kërkuara do të gjenden ndër të dhënat e OSHI-t dhe se këto

prova lidhen me veprën. Ky është i njëjti standard që zbatohet edhe për kontrollin e një banese apo biznesi në Shtetet e Bashkuara. Kërkesa duhet ë përmbajë detaje të mjaftueshme që përshkruajnë: (1) llojin e përmbajtjes që do të sekuestrohet (psh. komunikim me email) dhe (2) arsyen përse përmbajtja lidhet me veprën penale që po hetohet.

Informacioni “**aktual**” ose “i freskët” është kushti i dytë për të siguruar përmbajtjen e komunikimeve elektronike. Kjo do të thotë se të paktën disa prej fakteve ku bazohet kërkesa duhet të jenë relativisht të freskëta ose të tregojnë se ka të ngjarë që provat gjenden ende në vendin ku do të kërkohet. Gjykatat do ta refuzojnë një kërkesë nëse informacioni i paraqitur në të është i vjetër apo “i ndenjtur.” Megjithëse kjo duhet vlerësuar rast pas rasti (dhe nuk është një rregull i ngurtë), faktet që janë më të vjetra se 60 – 180 ditë, në kontekstin e provave elektronike, ka shumë të ngjarë të konsiderohen të “ndenjura”.

Nëse është dërguar një kërkesë për ruajtjen e informacionit më parë dhe vetëm tani shteti i huaj po kërkon t’i marrë këto të dhëna, ka shumë mundësi që problemi i vjetërsisë në kohë të tejkalohet pasi të dhënat mund fare mirë të ekzistojnë ende. Për më tepër, në disa raste si ato të pornografisë me të miturit, ato që zakonisht do të quheshin të dhëna të vjetra, gjykatat amerikane i kanë quajtur ende të “freskëta”. Nëse keni shqetësimin se mos kërkonit prova të vjetra në një çështje të caktuar, ju lutemi kontaktoni fillimisht me autoritetet amerikane para se të dërgoni kërkesën.

### **Shembuj ku përmbajtja mund të jetë e dobishme ose e rëndësishme**

Rasti hipotetik nr. 1 (shfrytëzim i të miturve)

Në rastin kur Viktorias 12-vjeçare iu kërkua të udhëtonte për të takuar “Xhonë,” Xhoja i dërgon email viktimës ku i thotë se një “miku” i tij i kishte lënë një mesazh zanor ku i kërkonte që Viktoria dhe Xhoja ta takonin në një vend të caktuar pas një jave në orën 3 pasdite. Hetuesi dëshiron të sigurojë përmbajtjen e komunikimeve në llogarinë e emailit të “Xhosë” për të parë se me kë bashkëpunon ai dhe nëse Xhoja dhe miku i tij kanë diskutuar për planet që kanë pas mbërritjes së Viktorias.

Rasti hipotetik nr. 2 (kërcënim për marrje pasurie)

Në rastin kur Korporata ABC merr emailin kërcënues, hetuesi ka marrë të dhënat e transaksioneve në lidhje me hyrjet në faqen elektronike të të dyshuarit (ku është afishuar informacioni i klientit) dhe duket se një sërë adresash IP që lidhen me këto përdorime kanë dalë nga rrjeti i kompanisë ABC në Shtetet e Bashkuara. Hetuesi beson se kjo tregon që një person i brendshëm po bashkëpunon me personin që bën kërcënimet. Hetuesi tashmë dëshiron të sigurojë përmbajtjen e të gjitha emaileve në llogarinë e kërcënuesit për të identifikuar personin e brendshëm dhe për të verifikuar marrëdhënien e tyre. Si rezultat, hetuesi i kërkon Korporatës ABC të sigurojë dhe t'i paraqesë kopje të të gjithë përmbajtjes së llogarisë email të punonjësit.

### Rasti hipotetik nr. 3 (vjedhje e informacionit elektronik)

Në rastin kur paratë në bankën e gjyshes u vodhën nga një pirat elektronik, hetuesi ka mësuar se një javë më parë pirati i kishte dërguar një email me udhëzime bankës se ku t'i transferonte fondet në llogarinë e gjyshes. Hetuesi më parë kishte kërkuar që llogaria e emailit të piratit të ruhej dhe tani dëshiron të dijë përmbajtjen e të gjitha mesazheve në llogarinë e tij për të parë nëse edhe persona të tjerë janë viktimizuar në të njëjtën mënyrë, si edhe për të parë nëse pirati ka kontaktuar edhe banka të tjera për kërkesa të ngjashme.

## Llojet e përmbajtjeve të disponueshme

### Për llogaritë email ose të faqeve elektronike

- Përmbajtja e të gjitha emaileve të ruajtura në llogari, duke përfshirë kopje të emaileve të dërguara nga llogaria.

### Për llogari në rrjetet sociale

- Të gjitha komunikimet dhe mesazhet e dërguara apo të marra nga përdoruesi, ku përfshihen të gjitha mesazhet private dhe kërkesat në pritje për “Miq”.

<p><b>KËSHILLË PRAKTIKE:</b> Nëse shteti kërkues arrin të përmbushë kriteret për të siguruar përmbajtjen, të dhëna për transaksionet dhe/ose informacioni për abonentin mund të sigurohen</p>
---

nëpërmjet të njëjtit proces, pasi këto të dhëna kërkojnë një proces ligjor me standard më të ulët sesa vetë përmbajtja.

## 5. Mbledhje në kohë reale e informacionit pa përmbajtje

### **Çfarë është?**

Mbledhja në kohë reale e informacionit pa përmbajtje i referohet sigurimit të informacionit të dërguar apo marrë (psh. të dhëna që identifikojnë se kush e dërgon një email) ndërkohë që komunikimi është ende rrugës për në destinacion (Shënim: ky mekanizëm jep gjithashtu edhe adresën fillestare të IP-së për logimin). Ky informacion nuk përfshin përmbajtjen e emailit, ndonjë material të bashkëngjitur apo rreshtin e lëndës.

### **Standardi ligjor**

Për të siguruar informacion pa përmbajtje në kohë reale në emër të një shteti të huaj kërkues, organet amerikane të zbatimit të ligjit duhet të demonstrojnë faktet specifike që përcaktojnë se si të dhënat dhe informacionet e tjera të kërkuara lidhen dhe janë pjesë përbërëse e hetimit të çështjes. Me fjalë të tjera, shpjegoni se si informacioni i kërkuar lidhet me hetimin për të cilin kërkohet. Pasi gjykata nxjerr një vendim, organet amerikane të zbatimit të ligjit mund ta mbledhin këtë informacion në kohë reale deri në 60 ditë dhe ta përtërijnë kërkesën edhe për 60 ditë të tjera nëse është e nevojshme (dhe nëse miratohet nga gjykata). Ky informacion mund t'u jepet organeve të huaja të zbatimit të ligjit menjëherë.

### **Rast hipotetik ku informacioni pa përmbajtje e në kohë reale mund të jetë i dobishëm**

Hetuesi pret që i dyshuari të dërgojë një email nga një llogari e caktuar Yahoo brenda dy ditëve të ardhshme, i cili përmban një kërkesë për shpërblim. Hetuesi kërkon informacion në kohë reale për origjinën e emailit (dmth. adresën IP nga e cila dërguesi hyn në Yahoo) për të përcaktuar vendndodhjen fizike të të dyshuarit dhe, në rrethana ideale, për ta kapur atë.

**KËSHILLË PRAKTIKE:** Kjo teknikë është veçanërisht e dobishme kur objektivi lëviz shpesh nga një kompjuter tek një tjetër, si psh, nëpër internet kafe. Hetuesi i cili ka adresën e IP-së që ka përdorur i dyshuari dhe orën kur është përdorur, mund të jetë në gjendje të identifikojë vendndodhjen e individit.

## 6. Mbledhje në kohë reale e informacionit me përmbajtje

Praktika ligjore në Shtetet e Bashkuara përjashton mbledhjen në kohë reale të përmbajtjes së projektuar vetëm mbi bazën e kërkesës nga qeveri të huaja. Megjithatë ekziston një përjashtim nga ky rregull, nëse zhvillohet një hetim i përbashkët me një organ amerikan të zbatimit të ligjit.

## 7. Kufizimet për dhënie ndihme

Shtetet e Bashkuara mund ta shtyjnë për më vonë ndihmën ndaj një kërkesë të huaj nëse ekzekutimi i kërkesës do të ndërhynte tek një hetim apo ndjekje penale që është në proces e sipër në Shtetet e Bashkuara. Në këtë situatë, Shtetet e Bashkuara mund të vonojnë ekzekutimin ose përndryshe mund të vendosin kushte që, nëse pranohen nga një shtet tjetër, do të ruanin integritetin e çështjes në SHBA.

Për më tepër, Shteteve të Bashkuara mund t'ju duhet të refuzojnë ndihmën nëse ekzekutimi i kërkesës bie në kundërshtim me interesin publik të Shteteve të Bashkuara. Për shembull, nëse sjellja në fjalë është një veprimtari që do të mbrohej me Kushtetutën e Shteteve të Bashkuara, kërkesa për ndihmë mund të refuzohet. Në mënyrë specifike, Shtetet e Bashkuara mund ta refuzojnë një kërkesë për ndihmë nëse lidhet me përfshirjen e një individi në shprehjen (me shkrim, me gojë apo tjetër) që mbulohet nga e drejta e shprehjes së lirë sanksionuar nga Kushtetuta e Shteteve të Bashkuara (psh. gjuha e “urrejtjes” zakonisht mbrohet nga Kushtetuta, edhe pse konsiderohet e pakëndshme), me përjashtim të rastit kur jepen fakte që tregojnë se shprehja shkon përtej fjalës së lejuar e të mbrojtur (psh. gjuha e urrejtjes që përfshin thirrje për veprime të menjëhershme dhune). Meqënëse jo çdo shprehje mbrohet nga Kushtetuta e Shteteve të Bashkuara, ju lutemi këshillohuni me autoritetet amerikane për të verifikuar nëse mund apo jo të jepet ndihmë në një çështje të caktuar.