KIBERJINOYAT ISHLARIDA ELEKTRON DALILLARNI TEZKOR SAQLASH VA ALMASHISHDAGI XALQARO HUQUQIY MUAMMOLAR

Mirzanazarov Elbek Avazbek o'g'li
Jahon iqtisodiyoti va diplomatiya universiteti Xalqaro huquq magistranti.
ORCID: 0009-0004-7623-0598 +998935665229

https://doi.org/10.5281/zenodo.20466924

Annotatsiya. *Kiberjinoyatlar bugungi kunda davlat chegaralarini juda tez kesib o'tmoqda va ularni tergov qilish jarayonida zarur bo'ladigan raqamli izlar, ya'ni elektron dalillar, ko'pincha boshqa mamlakat hududida saqlanadi. Bunday dalillar o'z vaqtida saqlab qolinmasa, ular butunlay yo'qolib ketishi mumkin. Shu sababli, elektron dalillarni tezkor saqlash va davlatlar o'rtasida samarali almashish uchun xalqaro hamkorlik alohida ahamiyat kasb etadi. Mazkur maqolaning asosiy maqsadi — mamlakatlar o'rtasida elektron dalillarni shoshilinch tarzda saqlash va almashish jarayoniga to'sqinlik qilayotgan asosiy huquqiy muammolarni aniqlashdan iborat. Tadqiqot davomida Budapesht konvensiyasi, 2024-yilda qabul qilingan yangi BMT Kiberjinoyat konvensiyasi, Yevropa Ittifoqi qonunchiligi hamda turli xalqaro tashkilotlar hisobotlari kabi rasmiy manbalar o'rganilib, ular o'zaro taqqoslandi.*

Tahlillar natijasida to'rtta asosiy muammo aniqlangan. Birinchidan, o'zaro huquqiy yordamning an'anaviy tizimi raqamli dalillar bilan ishlash uchun haddan tashqari sekin ishlaydi. Ikkinchidan, davlatlar chet el hududida saqlanayotgan ma'lumotlarga kirish masalasida yagona yondashuvga ega emas. Uchinchidan, davlat suvereniteti bilan ma'lumotlarni saqlovchi xususiy kompaniyalar zimmasidagi majburiyatlar o'rtasida ziddiyat mavjud. To'rtinchidan, ko'plab davlatlarda zarur texnik imkoniyatlar va tayyorgarlik yetishmasligi sababli mavjud huquqiy mexanizmlardan to'liq foydalanilmayapti. Shu asosda, tadqiqot davlatlar o'rtasida o'zaro huquqiy yordam mexanizmlarini soddalashtirish, yangi xalqaro huquqiy hujjatlarni kengroq joriy etish hamda rivojlanayotgan mamlakatlarga texnik va institutsional yordamni kuchaytirish zarurligini asoslab beradi.

Kalit so'zlar: *elektron dalil, kiberjinoyat, o'zaro huquqiy yordam, Budapesht konvensiyasi, BMT Kiberjinoyat konvensiyasi, ma'lumotlarni saqlash.*

Аннотация. *Киберпреступления в современном мире стремительно пересекают государственные границы, а цифровые следы, необходимые для их расследования, то есть электронные доказательства, нередко хранятся на территории других государств.*

Если такие доказательства своевременно не сохранить, они могут быть утрачены безвозвратно. В этой связи международное сотрудничество приобретает особое значение для оперативного сохранения и эффективного обмена электронными доказательствами между государствами. Основная цель данной статьи заключается в выявлении ключевых правовых проблем, препятствующих срочному сохранению и обмену электронными доказательствами между странами. В ходе исследования были проанализированы и сопоставлены официальные источники, включая Будапештскую конвенцию, новую Конвенцию ООН о киберпреступности 2024 года, законодательство Европейского союза, а также отчёты международных организаций. В результате анализа были выявлены четыре основные проблемы. Во-первых, традиционная система взаимной правовой помощи оказывается слишком медленной для работы с цифровыми доказательствами. Во-вторых, государства не пришли к единому подходу в вопросе доступа к данным, хранящимся за рубежом.

В-третьих, существует противоречие между государственным суверенитетом и обязательствами частных компаний, владеющих и обрабатывающих данные. В-четвёртых, во многих странах из-за недостатка технических возможностей и подготовки по-прежнему не используется в полной мере существующий правовой инструментарий. На этой основе в статье обосновывается необходимость упрощения механизмов взаимной правовой помощи между государствами, более широкого внедрения новых международно-правовых инструментов, а также усиления технической и институциональной поддержки развивающихся стран.

Ключевые слова: *электронные доказательства, киберпреступность, взаимная правовая помощь, Будапештская конвенция, Конвенция ООН по киберпреступности, хранение данных.*

Abstract. *Cybercrime today rapidly crosses national borders, and the digital traces needed for its investigation—known as elektronic evidence—are often stored in other countries.*

If such evidence is not preserved in a timely manner, it may be lost permanently.

Therefore, international cooperation is essential for the prompt preservation and effective exchange of elektronic evidence. The main objective of this article is to identify the key legal challenges that hinder the urgent preservation and exchange of elektronic evidence between countries. The study analyzes and compares official sources, including the Budapest Convention, the new 2024 UN Convention on Cybercrime, European Union legislation, and reports of international organizations. The findings reveal four major problems. First, the traditional system of mutual legal assistance is too slow for handling digital evidence. Second, states have not reached a common approach regarding access to data stored abroad. Third, there is a conflict between state sovereignty and the obligations of private companies that store and process data. Fourth, many countries are still unable to fully utilize existing legal mechanisms due to a lack of technical capacity and preparedness. Based on these findings, the article argues for simplifying mutual legal assistance procedures, promoting the broader adoption of new international legal instruments, and increasing technical and institutional support for developing countries.

Keywords: *elektronic evidence, cybercrime, mutual legal assistance, Budapest Convention, UN Convention on Cybercrime, data retention.*

Kirish. Bugungi kunda deyarli barcha jinoyatlar kompyuterlar, mobil telefonlar va internetda axborot izlarini qoldirishi mumkin. Ushbu axborot elektron dalillar, e-dalillar yoki raqamli dalillar deb ataladi. Elektron xatlar, fotosuratlar, chat xabarlari, kirish yozuvlari, IP manzillar va hatto joylashuv ma’lumotlari jinoyatchini topishga yoki biror kishining aybsizligini isbotlashga yordam berishi mumkin.

Ammo kiberjinoyat an’anaviy jinoyatdan bir muhim jihati bilan farq qiladi: dalillar ko‘pincha ishni tergov qilayotgan politsiya xodimi bilan bir mamlakatda bo‘lmaydi.[1] Muammo shundaki, raqamli ma’lumotlar juda tez harakatlanadi va undan ham tezroq yo‘qolishi mumkin.

Jinoyatchi o‘z ma’lumotlarini uzoq mamlakatdagi serverda saqlaydigan elektron pochta xizmatidan foydalanishi mumkin. Haker hujumni uch yoki to‘rt xil davlatdagi qurilmalar orqali yo‘naltirishi mumkin.

[1] United Nations Office on Drugs and Crime (UNODC), *Cybercrime Module 6 Key Issues: Handling of Digital Evidence*, available at https://www.unodc.org/e4j/en/cybercrime/module-6/key-issues/handling-of-digital-evidence.html (accessed 15 April 2026).

“Bulut”da saqlangan ma’lumotlar bir necha soniya ichida bir ma’lumot markazidan boshqasiga ko‘chirilishi mumkin. Agar dalillar tezda xavfsiz holatga keltirilmasa, kompyuter tizimi tomonidan avtomatik ravishda yoki jinoyatchi tomonidan qasddan o‘chirib tashlanishi mumkin. “Bunday jinoyatlarning elektron dalillarini, ma’lumotlarning o‘zgaruvchanligi sababli, to‘plash qiyin bo‘lishi mumkin.”[2] Shuning uchun xalqaro huquqiy matnlar hozirda kompyuter ma’lumotlarini *tezkor saqlash* qoidalarini o‘z ichiga oladi. “Tezkor” juda tez degan ma’noni anglatadi. 2001 yilda imzolash uchun ochilgan Budapesht kiberjinoyat konvensiyasi internet orqali sodir etiladigan jinoyatlar bo‘yicha birinchi majburiy xalqaro shartnomadir.[3] Uning 16-moddasida har bir Tomon o‘z organlariga saqlanayotgan kompyuter ma’lumotlarini tezkor saqlashni buyurish imkoniyatini berishi kerakligi aytilgan. 29-modda bir mamlakat boshqa mamlakatdan o‘z hududida saqlanayotgan ma’lumotlar uchun xuddi shu ishni qilishni so‘rashiga ruxsat beradi.[4]

2024 yil dekabr oyida Birlashgan Millatlar Tashkiloti Bosh Assambleyasi yangi, chinakam global shartnomani qabul qildi. Uning to‘liq nomi uzun: Birlashgan Millatlar Tashkilotining kiberjinoyatga qarshi konvensiyasi; Axborot-kommunikatsiya texnologiyalari tizimlari yordamida sodir etiladigan ayrim jinoyatlarga qarshi kurashish va og‘ir jinoyatlarning elektron shakldagi dalillarini almashish bo‘yicha xalqaro hamkorlikni mustahkamlash.[5] Odamlar uni odatda BMT Kiberjinoyat konvensiyasi deb ataydi.

Ushbu shartnoma ham elektron dalillarni tezkor saqlash va almashishni o‘z markaziga qo‘yadi. “Elektron dalillarni to‘plash va almashish qobiliyati muzokaralarni boshqardi va yakuniy shartnomaning asosiy unsurlarini shakllantirdi.” [6] Biroq, real hayotda boshqa mamlakatdan elektron dalillarni olish sekin va muammolarga to‘la bo‘lib qolmoqda. Bir tadqiqot shunday deydi: “kiberjinoyat ishlarida o‘zaro huquqiy yordam so‘rovlarining bajarilishi sekin va samarasizligicha qolmoqda. Xalqaro tizimlardagi bo‘shliqlar elektron dalillarga qonuniy kirishga to‘sqinlik qilmoqda.”[7] Boshqa bir hisobot esa “til farqlari, bir-biriga to‘g‘ri kelmaydigan huquqiy tizimlar va milliy idoralarning yetarli texnik salohiyati yo‘qligi sababli tergovlar tez-tez kechikmoqda” deb izohlaydi.[8] Ushbu maqolaning maqsadi elektron dalillarni chegaralar orqali tezkor saqlash va almashishni juda qiyinlashtiradigan eng muhim huquqiy muammolarni aniqlashdir.

Shuningdek, ularni hal qilishning mumkin bo‘lgan yo‘llarini taklif etishga harakat qiladi.

Usullar. Ushbu tadqiqot normativ-huquqiy tahlil hisoblanadi. Bu degani, suhbatlar o‘tkazmasdan yoki raqamlarni to‘plamasdan, xalqaro va milliy qonunlarning yozma matnlarini ko‘rib chiqadi va ularni taqqoslaydi. Foydalanilgan barcha manbalar har kim internetda bepul topib o‘qiy oladigan rasmiy hujjatlardir.[9]

Asosiy manbalar quyidagilardir:

[2] UNODC, *Cybercrime Module 6 Key Issues*, as above.
[3] Council of Europe, *Convention on Cybercrime*, Budapest, 23.XI.2001, European Treaty Series No. 185.
[4] Budapest Convention, Articles 16 and 29.
[5] United Nations, *UN Convention against Cybercrime*, A/RES/79/…, adopted 24 December 2024.
[6] UNODC, *Cybercrime Module 6 Key Issues*, section on “International cooperation”.
[7] Naeem AllahRakha, “Jurisdiction and Due Process Challenges in Addressing Cross-Border Cybercrime,” *Jurnal ADLIYA*, vol. 18, no. 2, 2024, p. 45.
[8] Eurojust, *Challenges and best practices from Eurojust’s casework in the area of cybercrime*, October 2020, p. 12, available at https://www.eurojust.europa.eu.
[9] All official documents cited are available on the websites of the United Nations, the Council of Europe, the European Union, and UNODC.

1. **Budapesht kiberjinoyat konvensiyasi** (ETS 185, 2001 yil 23 noyabr), ayniqsa 16, 29, 30, 31, 32 va 35-moddalar.[10]

2. **Budapesht konvensiyasining Ikkinchi qo‘shimcha protokoli** (2022 yil may oyida qabul qilingan), u xizmat ko‘rsatuvchi provayderlar bilan bevosita hamkorlikni va qo‘shma tergov guruhlarini joriy etadi.[11]

3. **BMT Kiberjinoyat konvensiyasi** (A/RES/79/…, 2024 yil dekabrda qabul qilingan), xususan o‘zaro huquqiy yordam, saqlash va elektron dalillarga transchegaraviy kirish haqidagi bo‘limlar.[12]

4. **YI e-dalillar reglamenti** (Regulation (EU) 2023/1543) va hamroh Direktiva (Directive (EU) 2023/1544), ular Yevropa saqlash va taqdim etish buyruqlarini yaratadi.[13]

5. **AQSH CLOUD qonuni** (2018), bu AQSH huquqni muhofaza qilish organlariga ma’lum shartlar ostida chet elda saqlanayotgan ma’lumotlarga kirishga ruxsat beradi.[14]

6. **BMT Narkotiklar va jinoyatchilik bo‘yicha boshqarmasining (UNODC) elektron dalillar va kiberjinoyat bo‘yicha ta’lim modullari.[15]**

7. **Yevrojust, Yevropa Kengashi va boshqa xalqaro tashkilotlarning kiberjinoyat ishlaridagi muammolar va eng yaxshi amaliyotlar haqidagi hisobotlari.[16]**

Tadqiqot avval har bir matnni diqqat bilan o‘qiydi. So‘ngra, matnlarning o‘zi tilga olgan yoki mutaxassislar hisobotlarda tasvirlagan barcha huquqiy muammolarni ajratib oladi. Keyin bu muammolar to‘rtta katta mavzuga guruhlanadi. Muammolarga birgalikda qarab, tizim nima uchun yaxshi ishlamasligini va eng katta bo‘shliqlar qayerda ekanini tushunish osonroq bo‘ladi.

Natijalar. Tahlil kiberjinoyat ishlarida elektron dalillarni saqlash va almashishni sekinlashtiradigan bir-biri bilan bog‘liq to‘rtta huquqiy muammoni ochib beradi. Har bir muammo quyida tushuntiriladi.

1. O‘zaro huquqiy yordam (MLA) tizimi raqamli dalillar uchun juda sekin

Ko‘pincha MLA deb ataladigan o‘zaro huquqiy yordam bir davlatning jinoiy tergovda yordam so‘rab boshqa davlatga murojaat qilishining an’anaviy usulidir. Bu bir hukumatdan boshqasiga yuborilgan rasmiy so‘rov xatiga o‘xshaydi. Ko‘p o‘n yillar davomida bu yetarli edi, chunki dalillar odatda tez yo‘qolib ketmaydigan qog‘oz hujjatlar yoki jismoniy narsalar edi.[17] Jarayon markaziy idoralar, masalan, Adliya vazirligi orqali ishlaydi. Mahalliy politsiya xodimi so‘rov yozadi va uni milliy markaziy idoraga yuboradi.

U idora so‘rovni tarjima qiladi, tekshiradi va so‘ngra so‘ralgan davlatning markaziy idorasiga yetkazadi. So‘rov keyin shu davlatdagi mahalliy prokuror yoki sudyaga tushadi, u esa so‘rovni bajarish yoki bajarmaslik haqida qaror qabul qilishi kerak. Har bir qadam haftalar yoki oylar olishi mumkin. “Asosiy sabab – mavjud o‘zaro huquqiy yordam vositalarida belgilangan tartiblarning davomiyligi bo‘lib, ular kiberjinoyat va… elektron dalillarga qarshi kurashishni

[10] Council of Europe, *Convention on Cybercrime*, ETS 185, 2001.
[11] Council of Europe, *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, CETS 224, 12 May 2022.
[12] United Nations, *UN Convention against Cybercrime*, 2024.
[13] Regulation (EU) 2023/1543 on European Production and Preservation Orders, OJ L 191, 19.7.2023; Directive (EU) 2023/1544 on designated establishments and legal representatives, OJ L 191, 19.7.2023.
[14] Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Public Law 115-141, 23 March 2018, amending 18 U.S.C. § 2523.
[15] UNODC, *University Module Series: Cybercrime*, Module 6, available at https://www.unodc.org/e4j/cybercrime.
[16] See notably Eurojust, *Cybercrime Judicial Monitor*, Issue 5, 2019; Council of Europe, *T-CY Guidance Note #10 on production orders for electronic evidence*, 2021.
[17] AllahRakha, “Jurisdiction and Due Process Challenges,” p. 47.

maqsad qilganiga qaramay, ko‘pincha juda sekin bo‘lib chiqmoqda.” [18] Elektron dalillar “o‘zgaruvchan”. Bu degani, ular o‘zgarishi yoki juda tez o‘chirilishi mumkin. Internet xizmat ko‘rsatuvchi provayderlar ko‘pincha elektron xatlar yoki ulanish yozuvlari kabi ma’lumotlarni faqat cheklangan muddatga saqlaydi. Ko‘p uchraydigan muddat 30 dan 90 kungacha.[19] Agar MLA so‘rovi shu muddat o‘tgandan keyin yetib kelsa, ma’lumotlar abadiy yo‘qoladi. “Transchegaraviy so‘rov tartibi sikli bilan elektron dalillarni saqlash imkoniyat oynasi o‘rtasida tabiiy ziddiyat mavjud.”[20]

Bundan tashqari, ko‘plab MLA shartnomalarida “ikki tomonlama jinoiylik” degan qoida mavjud. Bu degani, xatti-harakat so‘rovchi mamlakatda ham, so‘ralgan mamlakatda ham jinoyat hisoblanishi kerak. Ba’zi mamlakatlar hali kiberxatti-harakatlarning ayrim turlarini jinoyat deb belgilamagan, shuning uchun shart bajarilmaydi va so‘rov rad etiladi. Budapesht konvensiyasi saqlash so‘rovlari uchun “ikki tomonlama jinoiylik bunday saqlashni ta’minlash sharti sifatida talab etilmaydi” deb belgilab, bu muammoni hal qilishga harakat qiladi. [21] Biroq, bu osonlashtirilgan qoida faqat konvensiyaga qo‘shilgan mamlakatlar o‘rtasida ishlaydi. Qisqasi, eski MLA mashinasi raqamli ma’lumotlar millisoniyalarda harakatlanib, yo‘qolishi mumkin bo‘lgan dunyo uchun emas, qog‘oz xatlar dunyosi uchun qurilgan.

2. Chet elda saqlanayotgan ma’lumotlar ustidan yurisdiksiya bo‘yicha bir-biriga zid da’volar

Ikkinchi katta muammo shundaki, mamlakatlar o‘z hududlaridan tashqarida saqlanayotgan elektron dalillarga kim tegishi mumkinligi borasida kelisha olmaydi. Xalqaro huquqning an’anaviy qoidasi hududiy suverenitetdir: davlat o‘z kuchini faqat o‘z chegaralari ichida ishlatishi mumkin.[22] Ammo bulutdagi ma’lumotlarning qat’iy jismoniy uyi yo‘q. U bir vaqtning o‘zida turli mamlakatlardagi ko‘plab serverlar bo‘ylab bo‘linib ketishi mumkin. Ayrim mamlakatlar, masalan, AQSH o‘zining CLOUD qonuni bilan “ma’lumotlarni nazorat qilish” yondashuvini tanladi. Bu degani, AQSH sudi AQSHda joylashgan texnologiya kompaniyasiga (masalan, elektron pochta provayderiga) ma’lumotlarni, hatto u boshqa mamlakatdagi serverda saqlangan bo‘lsa ham, topshirishni buyurishi mumkin.[23] Boshqa mamlakatlar, ayniqsa kuchli ma’lumotlarni himoya qilish qonunlariga ega bo‘lganlar, “ma’lumotlarning joylashuvi” yondashuvini afzal ko‘radi. Ular shunday deydi: ma’lumot jismonan qayerda saqlansa, faqat o‘sha davlatgina undan foydalanishga ruxsat berishi mumkin. Bu to‘g‘ridan-to‘g‘ri ziddiyatni keltirib chiqaradi: xizmat ko‘rsatuvchi provayder ikkita buyruq olishi mumkin, biri u joylashgan A mamlakatdan, biri esa ma’lumot turgan B mamlakatdan. Bir ekspert yozganidek, “bir davlatning qonuniga rioya qilish boshqasinikini buzishni taqozo etadi.”[24]

Budapesht konvensiyasining 32-moddasi davlatga boshqa mamlakatda saqlanayotgan ochiq ma’lumotlarga kirishga yoki uni oshkor qilish huquqiga ega bo‘lgan shaxsning roziligi bilan ma’lumotlarga kirishga ruxsat beradi.[25]

---

[18] Council of Europe, *Cybercrime: towards a new legal tool on electronic evidence*, 2016, p. 8.
[19] UNODC, *Cybercrime Module 6*, section “Data retention periods”.
[20] Council of Europe, *Cybercrime: towards a new legal tool on electronic evidence*, 2016, p. 8.
[21] Budapest Convention, Article 29(3).
[22] Malcolm N. Shaw, *International Law*, 8th ed., Cambridge University Press, 2017, p. 361. (Foundational principle, not electronic evidence specific.)
[23] CLOUD Act, § 3.
[24] Vanessa Franssen and Stanisław Tosza, “Unresolved Jurisdictional Issues in Law Enforcement Access to Data,” in *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, Cambridge University Press, 2025 (open access preprint), p. 12.
[25] Budapest Convention, Article 32.

Ammo bu modda ehtiyotkor murosa bo‘lib, barcha qiyin savollarga javob bermaydi.

Kengaytirilgan hamkorlik bo‘yicha Ikkinchi qo‘shimcha protokol xizmat ko‘rsatuvchi provayderlarga to‘g‘ridan-to‘g‘ri buyruqlar tizimini yaratish orqali ba’zi bo‘shliqlarni to‘ldirishga harakat qiladi, lekin ko‘plab mamlakatlar uni hali imzolamagan yoki ratifikatsiya qilmagan.[26] Yangi BMT konvensiyasi ham transchegaraviy kirish haqidagi qoidalarni o‘z ichiga oladi, lekin ular ataylab noaniq qilib qo‘yilgan, chunki muzokaralarda ishtirok etgan davlatlar kuchli va aniq qoida bo‘yicha oddiygina kelisha olmadilar.[27]

3. Davlat suvereniteti, xususiy sektor majburiyatlari va ma’lumotlarni himoya qilish o‘rtasidagi ziddiyat

Zamonaviy kiberjinoyat tergovlari katta darajada xususiy kompaniyalar qo‘lidagi ma’lumotlarga bog‘liq: internet xizmat ko‘rsatuvchi provayderlar, elektron pochta kompaniyalari, ijtimoiy media platformalari va bulut operatorlari. An’anaviy MLA tizimi faqat davlatdan davlatga ishlaydi. U xususiy kompaniyalar ko‘plab dalillarning qo‘riqchisi bo‘lgan voqelik uchun ishlab chiqilmagan.[28] Ishlarni tezlashtirish uchun yangi huquqiy vositalar xususiy kompaniyalarni bevosita jalb qilishga harakat qiladi.

Budapesht konvensiyasining Ikkinchi qo‘shimcha protokoli va YI e-dalillar reglamenti xizmat ko‘rsatuvchi provayderlar bilan “bevosita hamkorlik” deb ataladigan narsaga ruxsat beradi. YI qoidalariga ko‘ra, bir a’zo davlatdagi sudya yoki prokuror boshqa a’zo davlatdagi xizmat ko‘rsatuvchi provayderga to‘g‘ridan-to‘g‘ri yuboriladigan Yevropa saqlash buyrug‘ini chiqarishi mumkin. Provayder ma’lumotlarni zudlik bilan saqlashi kerak; shoshilinch vaziyatlarda esa ularni sakkiz soat ichida oshkor qilishi lozim.[29]

Ushbu yangi mexanizmlar ancha tezdir, lekin ular qiyin huquqiy savollarni ham keltirib chiqaradi.

Birinchidan, to‘g‘ridan-to‘g‘ri buyruq provayder joylashgan mamlakat qonunlariga zid kelishi mumkin. Masalan, u mamlakatda ma’lumotlarni himoya qilish yoki bank siri haqida qat’iy qoidalar bo‘lishi mumkin. Ikkinchidan, xususiy kompaniyalar sudya emas; ular xorijiy buyruqning qonuniy va mutanosib ekanligini sinchkovlik bilan tekshirish vakolatiga ega emaslar.

Uchinchidan, to‘g‘ridan-to‘g‘ri buyruqlarning ko‘payishi provayderlar turli buyruqlar orasida qolib ketadigan va asosiy huquqlar yaxshi himoya qilinmaydigan vaziyatga olib kelishi mumkin. “Xususiy ishtirokchilar ko‘pincha o‘z mijozlari oldidagi majburiyatlari va o‘z milliy qonunlariga ko‘ra, ayrim elektron ma’lumotlarning maxfiyligini saqlaydi, bu esa jinoiy yordam davomida noaniq majburiyatlarga olib keladi.” [30] BMT Kiberjinoyat konvensiyasi xizmat ko‘rsatuvchi provayderlarning rolini tan oladi, lekin u baribir eng ko‘p nazoratni har bir davlatga qoldiradi. Shuning uchun davlat hokimiyati, kompaniya majburiyatlari va shaxsiy ma’lumotlarni himoya qilish o‘rtasidagi ziddiyat uzoq vaqt davom etishi mumkin.

4. Imkoniyatlarning yetishmasligi va notekis amalga oshirish

Nihoyat, agar mamlakatlar ularni amalda qo‘llay olmasa, dunyodagi eng yaxshi qonunlar befoyda. Ko‘plab davlatlarda hali ham maxsus politsiya bo‘linmalari, raqamli sud-ekspertiza vositalari, 24 soatlik aloqa nuqtalari va Budapesht konvensiyasi yoki yangi BMT konvensiyasi kabi hujjatlarni qo‘llash uchun zarur bo‘lgan o‘qitilgan sudya va prokurorlar yetishmaydi.[31]

[26] Second Additional Protocol, CETS 224, Preamble and Articles 6-8.
[27] UN Cybercrime Convention, Article 34 (preservation and disclosure of stored computer data).
[28] Franssen and Tosza, “Unresolved Jurisdictional Issues,” p. 5.
[29] Regulation (EU) 2023/1543, Articles 3 and 8.
[30] AllahRakha, “Jurisdiction and Due Process Challenges,” p. 51.
[31] Eurojust, *Challenges and best practices*, p. 18.

“Til to‘siqlari, bir-biriga mos kelmaydigan qonunlar va milliy idoralarning cheklangan texnik tajribasi” asosiy to‘siqlar sifatida tez-tez tilga olinadi.[32] Budapesht konvensiyasining 35-moddasi har bir Tomondan kiberjinoyat tergovlarida zudlik bilan yordam ko‘rsatish uchun haftasiga yetti kun, kuniga 24 soat ishlaydigan aloqa nuqtasini tashkil qilishni talab qiladi.[33]

Nazariyada, ushbu tarmoq har qanday Tomon mamlakatdagi politsiya xodimiga boshqa Tomon mamlakatdagi hamkasbiga qo‘ng‘iroq qilish va ma’lumotlarni bir necha soat ichida saqlatish imkonini berishi kerak. Amalda, hatto konvensiyaning 70 dan ortiq Tomonlari orasida ham, hammasi ham ishlaydigan 24/7 tarmoqqa ega emas. Ba’zi aloqa nuqtalari faqat ish soatlarida javob beradi. Boshqalarida esa tezkor harakat qilish uchun kompyuter uskunasi yetishmaydi. Yevrojust, Yevropa Ittifoqining sud hamkorlik organi, “ma’lumotlar tegishli qoidalarga muvofiq to‘planishini ta’minlash uchun kiberjinoyat operatsiyalariga sud organlarining erta jalb etilishi” hali ko‘p joylarda yetishmayotganini qayd etgan.[34] Yangi BMT konvensiyasi texnik yordam va imkoniyatlarni oshirish haqida gapiradi, ammo bu pul va siyosiy irodaga bog‘liq.[35] Politsiya uchastkalari va sudlarda asosiy imkoniyatlarsiz, elektron dalillarni tezkor saqlash faqat qog‘ozdagi go‘zal va’da bo‘lib qoladi.

Muhokama. Yuqorida tasvirlangan to‘rtta muammo bir-biri bilan chuqur bog‘langan.

Ularning barchasi bitta katta tarkibiy ziddiyatdan kelib chiqadi: jinoiy qonunchilik hali ham davlat hududi g‘oyasi atrofida tashkil etilgan, ammo kiberjinoyat chegaralarni e’tiborsiz qoldiradigan global hodisadir. Eski MLA tizimi 19-asrda dalil tortmasida qulflangan imzolangan hujjat bo‘lgan dunyo uchun qurilgan. Raqamli dalil esa oylar emas, balki soatlar yoki daqiqalar ichida harakat qilishni talab qiladi. Bir nechta qisman yechimlar allaqachon paydo bo‘la boshlagan. Birinchidan, YI e-dalillar to‘plami kabi mintaqaviy tajribalar shuni ko‘rsatadiki, bir a’zo davlatning sud buyrug‘i boshqasida bevosita ta’sir ko‘rsatadigan huquqiy maydonni yaratish mumkin. Regulation (EU) 2023/1543 “jinoiy tergovlarda elektron dalillarni olish bo‘yicha transchegaraviy hamkorlik uchun huquqiy asosni yaratadi” va bajarilishi majburiy bo‘lgan Yevropa saqlash buyruqlarini yaratadi.[36] Qisqa muddatlar (odatda o‘n kun, favqulodda holatlarda sakkiz soat) elektron dalillarning o‘zgaruvchanligiga to‘g‘ridan-to‘g‘ri javob beradi.

Ikkinchidan, Budapesht konvensiyasining Ikkinchi qo‘shimcha protokoli ikkita muhim yangilikni olib keladi: u qat’iy kafolatlar ostida prokurorlar va boshqa mamlakatlardagi xizmat ko‘rsatuvchi provayderlar o‘rtasida bevosita hamkorlikka ruxsat beradi va chegaralar bo‘ylab yagona birlik sifatida harakat qila oladigan qo‘shma tergov guruhlarini tuzishga imkon beradi.[37]

Ushbu vositalar tizimni asta-sekin sof hukumatdan-hukumatga modelidan uzoqlashtirmoqda. Uchinchidan, BMT Kiberjinoyat konvensiyasi, ko‘plab murosasizliklariga qaramay, ushbu mavzu bo‘yicha birinchi chinakam universal shartnomadir. U barcha 193 BMT a’zo davlatlariga umumiy til berishi mumkin. Konvensiyada “Ishtirokchi-davlatlar bir-biriga elektron dalillarga nisbatan eng keng o‘zaro huquqiy yordamni ko‘rsatadilar” deyilgan va u asosiy maqsadlari qatoriga texnik yordam va imkoniyatlarni oshirishni kiritadi.[38] Bu Budapesht konvensiyasi doirasidan hozirgacha chetda qolib kelgan mamlakatlar uchun umidli yo‘l yaratadi.

[32] UNODC, *Cybercrime Module 6*, section “Key challenges”.
[33] Budapest Convention, Article 35.
[34] Eurojust, *Cybercrime Judicial Monitor*, Issue 5, 2019, p. 22.
[35] UN Cybercrime Convention, Article 60 (Technical assistance).
[36] Regulation (EU) 2023/1543, Recital 3.
[37] Second Additional Protocol, Articles 9 and 10.
[38] UN Cybercrime Convention, Article 28(1) and Article 2(b).

Shunga qaramay, ushbu vositalar sehrli tayoqcha emas. Ularning barchasi umumiy zaif jihatga ega: ular davlatlarning hamkorlik qilishga siyosiy tayyorligiga bog‘liq. Davlat deyarli har doim so‘rovni rad etish uchun asos topishi mumkin, masalan, so‘ralgan harakat uning suverenitetiga, xavfsizligiga yoki jamoat tartibiga zarar yetkazadi deb aytish orqali.[39] Bugungi dunyoda siyosiy munosabatlar ko‘pincha keskin bo‘lgan bir paytda, kiberjinoyat bo‘yicha hamkorlik osonlikcha katta mojarolarning qurboniga aylanishi mumkin. Bundan tashqari, huquqiy manzara juda parchalanib ketgan. Bir vaqtning o‘zida bizda Protokollari bilan Budapesht konvensiyasi, yangi BMT konvensiyasi, batafsil YI qoidalari, AQSH CLOUD qonuni, ko‘plab ikki tomonlama bitimlar va paydo bo‘layotgan OECD tamoyillari mavjud. Bir akademik buni “xavfsizlik ehtiyojlari, shaxsiy hayot daxlsizligi huquqlari va yurisdiksiya muammolarini muvozanatlashtiruvchi majburiyatlarning murakkab tarmog‘i” deb ataydi.[40] 100 ta mamlakatda faoliyat yuritadigan texnologiya kompaniyasi uchun, u xorijiy hokimiyatdan saqlash so‘rovini olganida qaysi qoidaga rioya qilishni bilish deyarli imkonsiz bo‘lishi mumkin.

Ushbu chalkashlik jinoyatchilikka qarshi kurashga ham, foydalanuvchilarning ishonchiga ham zarar yetkazadi. Tadqiqot to‘rtta amaliy qadamning kombinatsiyasini taklif qiladi:

1. Tartibiy soddalashtirish. Davlatlar imkon qadar saqlash buyruqlarini to‘g‘ridan-to‘g‘ri yuborish modelini qabul qilishlari kerak. To‘rt yoki besh idoradan o‘tish o‘rniga, saqlash buyrug‘i so‘rovchi organdan to‘g‘ridan-to‘g‘ri ma’lumotlarni ushlab turadigan shaxs yoki kompaniyaga borishi kerak. YI e-dalillar reglamenti boshqa mintaqalarda ko‘chirilishi mumkin bo‘lgan yaxshi namunadir.[41]

2. 24/7 tarmog‘ini mustahkamlash. Har bir davlat Budapesht konvensiyasi va yangi BMT konvensiyasi talab qilganidek, yaxshi o‘qitilgan, doimiy mavjud bo‘lgan aloqa nuqtasini belgilashi kerak. Bu aloqa nuqtalari katta idoralar bo‘lishi shart emas; to‘g‘ri texnologiyaga ega kichik mutaxassislar jamoasi katta farq qilishi mumkin. Xalqaro tashkilotlar kichikroq davlatlarga ushbu aloqa nuqtalarini tashkil qilish va saqlashda yordam berishi kerak.[42]

3. Rivojlanayotgan mamlakatlarda imkoniyatlarni oshirish. Rivojlangan davlatlar va UNODC, Interpol, Yevropa Kengashi kabi xalqaro tashkilotlar politsiya xodimlari, prokurorlar va sudyalarni elektron dalillar bilan ishlashga o‘qitish uchun ko‘proq mablag‘ sarflashlari kerak. Huquqiy asos, agar undan foydalanishi kerak bo‘lgan odamlar IP manzil qanday ishlashini yoki serverni qanday xavfsiz holatga keltirishni tushunmasa, befoyda.[43]

4. Xususiy sektor uchun aniqroq xalqaro qoidalar. Davlatlar ma’lumotlar uchun transchegaraviy buyruqlarni qabul qiladigan xususiy kompaniyalar uchun umumiy minimal kafolatlar va tartiblar to‘plami ustida kelishish uchun birgalikda ishlashlari kerak. Bunday kelishilgan xulq-atvor kodeksi bir-biriga zid keladigan majburiyatlar sonini kamaytiradi va foydalanuvchilarning asosiy huquqlarini himoya qilishga yordam beradi. Uni yangi BMT konvensiyasi soyaboni ostida muhokama qilish mumkin.[44]

Xulosa. Elektron dalillarni tezkor saqlash va almashish kiberjinoyatga qarshi kurashdagi eng dolzarb ehtiyojlardan biridir. Ushbu maqola mavjud xalqaro huquqiy tizim ushbu ehtiyojni qondirish uchun hali ham juda sekin, juda parchalangan va hududiy suverenitet haqidagi eski g‘oyalarga qattiq bog‘lanib qolganini ko‘rsatdi.

[39] UN Cybercrime Convention, Article 30(2).
[40] AllahRakha, “Jurisdiction and Due Process Challenges,” p. 43.
[41] Regulation (EU) 2023/1543, Articles 3-5.
[42] Budapest Convention, Article 35; UN Cybercrime Convention, Article 40 (24/7 network).
[43] UNODC, *Cybercrime Module 6*, section “Capacity building and training”.
[44] This idea is discussed in Franssen and Tosza, “Unresolved Jurisdictional Issues,” p. 19.

An’anaviy o‘zaro huquqiy yordam tartiblari raqamli asr uchun ishlab chiqilmagan. Turli mamlakatlar bir xil ma’lumotlar ustidan turli xil vakolatlarga da’vo qiladilar. Xususiy kompaniyalardan sudya rolini o‘ynash so‘raladi, lekin ularda buning uchun huquqiy aniqlik yetishmaydi. Va ko‘plab davlatlar hali ham mavjud huquqiy vositalardan foydalanish uchun zarur bo‘lgan asosiy texnik imkoniyatlarga ega emas. Budapesht konvensiyasi va uning protokollari, yangi BMT Kiberjinoyat konvensiyasi va Yevropa Ittifoqining e-dalillar reglamenti kabi mintaqaviy islohotlar oldinga qo‘yilgan muhim qadamlardir. Ular tezkor harakat qilish uchun huquqiy vositalarni taqdim etadi.

Biroq, bu vositalar faqat davlatlar ularni haqiqiy siyosiy majburiyat bilan amalga oshirsa, xalqaro hamkorlik boshqa siyosiy kurashlar bilan to‘sib qo‘yilmasa va jahon hamjamiyati zarur infratuzilma va tayyorgarlikka jiddiy sarmoya kiritsagina samarali bo‘ladi. Kiberjinoyatchilar diplomatik notalarni kutib o‘tirmaydi. Qonun o‘zi himoya qilmoqchi bo‘lgan ma’lumotlar kabi tez harakat qilishni o‘rganishi kerak.

Foydalanilgan adabiyotlar:

1. Council of Europe, *Convention on Cybercrime* (ETS 185), Budapest, 23 November 2001.
2. Council of Europe, *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of elektronic evidence* (CETS 224), Strasbourg, 12 May 2022.
3. Council of Europe, *Cybercrime: towards a new legal tool on elektronic evidence*, 2016.
4. Eurojust, *Challenges and best practices from Eurojust’s casework in the area of cybercrime*, 2020.
5. Eurojust, *Cybercrime Judicial Monitor*, Issue 5, 2019.
6. Franssen, V. and Tosza, S., “Unresolved Jurisdictional Issues in Law Enforcement Access to Data,” in *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, Cambridge University Press, 2025 (open access preprint).
7. Naeem AllahRakha, “Jurisdiction and Due Process Challenges in Addressing Cross-Border Cybercrime,” *Jurnal ADLIYA*, vol. 18, no. 2, 2024.
8. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for elektronic evidence.
9. Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 on designated establishments and legal representatives.
10. United Nations, *United Nations Convention against Cybercrime* (A/RES/79/…), adopted December 2024.
11. United Nations Office on Drugs and Crime (UNODC), *University Module Series: Cybercrime*, Module 6, *Handling of Digital Evidence*, 2025.
12. U.S. Congress, *Clarifying Lawful Overseas Use of Data (CLOUD) Act*, Public Law 115-141, 2018.