Musayev E.♦

DOI: 10.25108/2304-1730-1749.iolr.2026.84.96-103
UDC: 343.3:004

Objective Elements of Criminal Offences and Causation in the Digital Environment

Abstract: The article examines the conditions under which technical changes caused by digital interference constitute legally significant results under Azerbaijani criminal law and can be attributed to conduct. The study aims to identify the boundaries between a technical event, factual causation and legal assessment. It combines formal legal and doctrinal analysis with problem-focused comparison. Azerbaijani legislation and selected judicial positions are compared with legislative, judicial and scholarly materials from Germany and the United States. The article does not automatically transfer foreign solutions into national law, makes no statistical generalisations and uses technical examples as hypothetical models. The analysis shows that alteration of data, interference with a system's operation, impairment of authenticity and loss of property are distinct legal results. A harm requirement not specifically imposed by law should not be added to the elements of an offence, and a required result should not be replaced by a description of danger. In cases involving multiple interventions, the analysis distinguishes a jointly produced result, independently sufficient causes and evidential uncertainty in identifying the person who caused the result. The unit of analysis is determined from conduct attributed to a person on the basis of evidence, before focusing on an individual packet. Another finding is that a system's vulnerability and a third party's subsequent decision do not automatically break the causal link. In cases of omission, technical ability does not replace a legal duty to act. The basis of that duty and whether the specific result could have been prevented are examined separately. An expert's technical finding does not replace the legal conclusion on whether the elements of an offence are satisfied and on fault. The article proposes a sequential assessment of individual conduct, the factual mechanism, alternative causes and legal attribution. The value of the approach lies in clarifying the questions answered by digital evidence and preserving the statutory limits of liability. The proposal does not create a new general offence and is not presented as an empirically validated model. The article shows that difficulties of interpretation, insufficient evidence and a genuine legislative gap must be distinguished before legislation is amended.

Keywords: legality; data integrity; service availability; multiple causation; omission; electronic evidence; expert opinion; individual liability.

Introduction

In digital interference, issuing a command, executing a program, altering data, interrupting a service and causing subsequent harm occur at different stages. Their sequence is not sufficient to attribute all the consequences to the same person. The article asks: under what conditions does a technical effect constitute the result required by an offence and become linked to specific conduct? The aim is to establish the justified limits of this transition in Azerbaijani criminal law. The central

♦ **Musayev Erkin** - Doctoral student, Department of Criminal Law and Criminology, Baku State University (Azerbaijan). Email: musayev2022@gmail.com

argument is that the technical event, factual causation and legal attribution of the result must be examined separately.

The study is based on formal legal, doctrinal and problem-focused comparative analysis. Azerbaijani provisions and selected judicial positions are compared with German and United States materials. The foreign sources have been selected to distinguish problems of causation, rather than to transfer grounds of liability into domestic law. No statistical generalisation or testing is undertaken. The examples concerning traffic flows and a system administrator are hypothetical. The proposed contribution is a sequential examination of the applicable provision, individual conduct, the factual mechanism, alternative causes and legal attribution.

1. Technical Change and the Result Required by Law

Under Articles 3 and 5 of the Criminal Code of the Republic of Azerbaijan (CC), liability requires all the statutory elements of the offence, and the application of criminal law by analogy is prohibited [3, Arts. 3, 5.1–5.2]. The analysis must therefore begin with the specific statutory definition rather than a general description of a cyberthreat. The target of interference must also be distinguished from harm to the protected relationship: an electronic record may be a target of interference, a means leading to property loss and a piece of evidence. These functions require separate legal justification.

H.R. Jafarov identifies conduct as a necessary element of all offences, while distinguishing the result and causation as necessary elements of result-based offences [5, pp. 7–8]. The Constitutional Court's decision of 7 January 2021 concerning Article 332.3 of the CC also distinguishes conduct-based and result-based offences in this respect [2, reasoning]. When the general distinction stated in the decision is applied to a specific digital act, the relevant statutory definition must provide the basis. The existence of a technical trace does not introduce a harm requirement that the provision does not separately impose.

Article 271.1 of the CC does not require separate property loss or disruption of a system's operation. However, the absence of a right of access, the alternative additional conditions in the statutory definition and intent must be examined [3, Art. 271.1]. A recorded connection attempt may not show that access actually occurred. Article 273.1 of the CC, by contrast, requires the listed forms of interference with data to cause significant harm; paragraph 1 of the Note defines this as damage exceeding one thousand manats or other substantial harm to interests protected by law [3, Art. 273.1 and Note, para. 1]. Deletion of a file, the resulting harm and the statutory threshold are separate matters for examination.

Article 273.2 of the CC concerns serious hindrance to a system's operation. Under paragraph 2 of the Note, a substantial restriction of the ability to use the system or exchange information with other systems must be assessed [3, Art. 273.2 and Note, para. 2]. Functional impairment must be established even where no financial loss is shown; a complete shutdown is not the only criterion. Under the proposed approach, the restricted function, duration and intensity are substantiated in relation to the system's purpose. A uniform threshold measured in seconds or traffic volume does not replace the statutory criterion of significance. The impairment of authenticity under Article 273-2 of the CC also differs from unavailability: data may remain readable while being falsified. The purpose of presenting or using false data as authentic must also be examined separately [3, Art. 273-2].

The German Criminal Code (StGB) addresses interference with data, significant disruption of important data processing and property loss caused by influencing processing in separate offences [8, §§ 303a(1), 303b(1), 263a(1)]. The 2024 official edition of United States law likewise distinguishes

"damage", denoting impairment of integrity and availability, from "loss", which includes response, assessment and restoration costs and economic losses arising from service interruption [9, § 1030(e)(8), (11)]. The author's proposal drawn from this comparison is to distinguish restoration costs from expenditure on upgrading the system beyond its previous condition. No expenditure is excluded in advance. Its connection with the interference and its necessity must be substantiated.

In Pulte Homes, allegations that numerous calls and messages had reduced communication capacity were examined. The United States Court of Appeals for the Sixth Circuit reinstated the transmission claim, while finding that unauthorised access had not been sufficiently alleged in relation to the use of open communication channels [10, opinion, pp. 6–8, 10–12]. This was a review of the initial dismissal of a civil claim, and the facts were assumed to be true at that stage. The decision does not establish criminal fault; it shows that functional harm is not the same element as unauthorised access. Under domestic law, each result must be established according to its own statutory definition.

2. Factual Causation and Multiple Interventions

The initial question of factual causation is whether the particular result would have occurred in those circumstances without the person's conduct. The "conditio sine qua non" approach examines the result by mentally removing the conduct. Moore explains the traditional distinction between factual and legal causation and its disputed boundaries [6, §§ 2.1–2.3]. Temporal proximity does not replace the causal mechanism. Each link between blocking data, delaying an operation and financial loss requires separate proof. Jafarov likewise explains that temporal sequence is insufficient [5, pp. 9–10]. Establishing the factual connection is not proof of fault, and the CC excludes liability for harm caused without fault [3, Arts. 7.1–7.2].

In Burrage v. United States, the expert conclusion that heroin had contributed to death together with other substances did not establish that it was a necessary cause. Under the particular federal drug provision, and where an independently sufficient cause had not been proved, the United States Supreme Court applied the necessary-cause requirement, reversed the conviction on the second count and remanded the case [11, pp. 206–211, 218–219]. This was neither a complete acquittal nor a cybercrime decision. The Court neither accepted nor rejected a special rule for independently sufficient concurrent causes [11, p. 215]. A necessary cause therefore does not mean the sole cause, and the decision does not establish a universal rule of digital causation.

Disruption of a service through numerous requests allows three situations to be distinguished. In the first, each of two traffic flows remains below a harmful threshold on its own, but together they cause a serious hindrance. In the second, each flow is independently sufficient to produce the result, and both actually contribute to it. In the third, only one intervention caused the result, but which one remains unidentified. A result produced jointly, concurrent sufficient causes and failure to establish through evidence which intervention caused the result are not the same problem. Resolving them under the single label "multiple causation" would conflate actual causal contribution with evidential uncertainty.

The "NESS" approach presented by Moore seeks a necessary element within a set of conditions sufficient for the result and shows the limitations of the simple removal test in cases of concurrent causes [6, §§ 5.1.1–5.1.2]. A theoretical criterion does not, however, determine the unit of conduct by itself. Requiring each packet to be necessary on its own may distort the legal assessment of a large-scale attack, but this does not imply liability for every technical participant. The unit of analysis is specific conduct attributed to a person through evidence. A continuous flow controlled by one person must not be combined without justification with flows generated by people unaware of one another.

Complicity cannot be inferred merely from targeting the same system, nor can it fill a gap in the proof of causation.

3. Legal Attribution, Subsequent Conduct and Omissions

Once factual causation has been established, the legal significance of the result must be examined. Developing a program or opening an account may be among the conditions that lead to later harm. Treating all such conditions as causes for the purposes of criminal law would extend liability without clear limits. Legal attribution here means explaining how the factual effect relates to the conduct prohibited by the provision and the interest it protects. It does not create a new ground of liability. The objection that requiring a clearly established causal link may weaken protection in complex systems should be considered. However, replacing the specific result required by law with an increase in risk would change the structure of the offence. Difficulty of proof does not remove a statutory element.

A pre-existing vulnerability does not, by itself, break the link between the attack and the result. Nor can it be presumed that every person who breached a security rule caused that result. The way in which the exploited vulnerability affected the result must be established. The absence of a backup may not cause the initial deletion, but it may affect the possibility of recovery. The occurrence of harm and its increase are separate questions. Subsequent human conduct does not automatically break the link either. Under Article 178.1 of the CC, the transfer of property by a person deceived through phishing may form part of the deception mechanism [3, Art. 178.1]. An independent later decision and an automated operation must, however, be assessed separately.

Peters first examines the link between the encryption of a hospital system and a patient's death by asking whether earlier treatment would have saved the patient's life. He then analyses the diversion to another hospital as a response to the initial danger [7, pp. 17–18]. This is a conditional doctrinal model, not a judicial finding on the cause of death. The model shows that interruption of a service and loss of life raise different questions of causation. Not every response should be treated as a continuation of the initial interference: whether it reduces the earlier danger, creates an independent new risk or affects the final result must be distinguished. An error in the response does not automatically mean that the causal link is broken.

In cases of omission, technical ability must be distinguished from a legal duty. Jafarov's medical example examines both the objective possibility of providing assistance and whether it would prevent the result [5, p. 16]; a medical duty cannot be equated with an administrator's duty. Section 13(1) of the German Criminal Code (StGB) requires a legal obligation to prevent the result and equivalence between the omission and commission of the offence through a positive act [8, § 13(1)]. This foreign rule does not mean that the same general provision exists in national law. A contract or an instruction may clarify a duty, but it does not replace the statutory elements of an offence. Negligent conduct is also an offence only in the cases provided for in the Special Part [3, Arts. 3, 5.1–5.2, 24.2].

If, hypothetically, an administrator fails to intervene despite a warning, the content of the warning, the administrator's authority, the ability to act and the timing of any possible measure must be established. The next question is whether the required measure would have prevented the particular result in dispute. If the measure became possible only after the result occurred, the failure to take it earlier cannot be treated as the cause of that result. If the attack exploited another vulnerability that the measure would not have addressed, a link between a general breach of duty and the specific harm must not be presumed. The source of the duty, the possibility of prevention and the applicable offence require separate justification.

4. The Limits of Moving from Evidence to Legal Assessment

A log may show the time and technical address of an operation, while analysis of a program may reveal how it produced an effect. The reliability of the data, attribution of conduct to a person and whether the result arose from that conduct are not interchangeable questions. A link between an account and a person does not show that the person performed every operation. The rules of the Code of Criminal Procedure on matters to be proved and the assessment of evidence provide a basis for this distinction [4, Arts. 139.0.1–139.0.4, 145]. An expert opinion has no predetermined superior evidential weight [4, Arts. 127.3, 144–145].

Resolution No. 5 of the Plenum of the Supreme Court, dated 15 November 2013, emphasises that questions of guilt and legal assessment must not be entrusted to an expert [1, paras. 19–20]. The guidance concerns transport cases and is used here only as a methodological comparison. An expert may examine which command changed which data and whether an alternative malfunction explains the result. The court, however, must explain whether the change meets the statutory threshold of 'significant harm' or 'serious hindrance'. This does not diminish the expert's role; it makes the transition from a technical finding to a legal conclusion clear.

Where the result required by law has not been established, the basis for finding a completed offence is also limited. Article 27.1 of the CC links completion to the presence of all the elements of the offence, while Article 29 sets out separate conditions for attempt [3, Arts. 27.1, 29]. The start of an attack does not show that a serious hindrance has occurred. Conversely, the absence of a result does not automatically mean either an absence of liability or an attempt: the stage of execution, what the conduct was directed towards and the existence of another completed offence must be examined separately. This distinction prevents gaps in the facts from being filled by legal assumptions.

Jafarov's proposal for a general statutory definition of causation may promote consistency in terminology [5, p. 8]. Nevertheless, a definition cannot itself resolve questions involving different results, parallel causes or the source of a duty in cases of omission. Before a legislative proposal is made, it is necessary to determine whether the problem arises from interpretation, insufficient evidence or a genuine gap in the law. The need for a new provision can be justified only after this distinction has been made.

Conclusion

Five stages are proposed for assessing a digital result: identifying the specific provision and the result it requires, the conduct attributed to the person, the factual mechanism that produced the result, alternative and concurrent causes, and the legal attribution of the factual effect within the limits of that provision. This sequence helps distinguish harm, functional disruption and changes in authenticity, and prevents technical involvement from being treated as a substitute for causation. Fault and complicity are assessed separately. The practical usefulness of the model should be tested through its subsequent application to selected cases; no empirical validation is claimed here.

No firm conclusion is drawn on the need for a new general provision. When existing offences are applied, technical uncertainty must not be resolved by legal assumptions. The selected judicial materials do not represent national practice as a whole, and foreign approaches cannot provide grounds for extending the elements of offences under Azerbaijani legislation.

References

1. Plenum of the Supreme Court of the Republic of Azerbaijan. On judicial practice regarding criminal cases concerning violations of traffic and vehicle operation rules. November 15, 2013, Resolution No. 5. Available at: https://supremecourt.gov.az/storage/pages/535/26-yol-hereketi-ve-neqliyyat-vasitelerinin-istismari-qaydalarinin-pozulmasina-dair.pdf. (In Azerbaijani).

2. Plenum of the Constitutional Court of the Republic of Azerbaijan. On the interpretation of Article 332.3 of the Criminal Code of the Republic of Azerbaijan. Resolution, January 7, 2021. Available at: https://constcourt.gov.az/az/decision/1202. (In Azerbaijani).

3. Criminal Code of the Republic of Azerbaijan. Approved by Law No. 787-IQ dated December 30, 1999. Official consolidated text. Available at: https://frameworks.e-qanun.az/46/f_46947.html. (In Azerbaijani).

4. Criminal Procedure Code of the Republic of Azerbaijan. Approved by Law No. 907-IQ dated July 14, 2000. Official consolidated text. Available at: https://frameworks.e-qanun.az/46/f_46950.html. (In Azerbaijani).

5. Jafarov H.R. Issues regarding causal connection in criminal law: abstract of the dissertation for the degree of Doctor of Philosophy in Law. Baku: Baku State University, 2014. 27 p. Available at: https://aak.gov.az/upload/dissertasion/huq/huq_n_chr_30_05_14.pdf. (In Azerbaijani).

6. Moore M. Causation in the Law. The Stanford Encyclopedia of Philosophy. Spring 2024 ed. / Eds. E.N. Zalta, U. Nodelman. Stanford: Metaphysics Research Lab, 2024. Available at: https://plato.stanford.edu/archives/spr2024/entries/causation-law/.

7. Peters K. Cyberkriminalität im aktuellen Strafrecht. In: Peters K. (Hrsg.). Cyberkriminalität. Aktuelle Herausforderungen für Polizei, Staatsanwaltschaft, Gerichte und Wissenschaft. München: LMU, 2022. S. 1–28. DOI (məcmuə): 10.5282/ubm/epub.92172. Available at: https://epub.ub.uni-muenchen.de/92172/1/Peters_Cyberkriminalitaet.pdf.

8. Strafgesetzbuch. Neufassung vom 13.11.1998, BGBl. I S. 3322. Gesetze im Internet: konsolidierte Fassung. Available at: https://www.gesetze-im-internet.de/stgb/BJNR001270871.html.

9. United States Code. Title 18, § 1030: Fraud and related activity in connection with computers. 2024 Edition. U.S. Government Publishing Office. Available at: https://www.govinfo.gov/content/pkg/USCODE-2024-title18/html/USCODE-2024-title18-partI-chap47-sec1030.htm.

10. United States Court of Appeals for the Sixth Circuit. Pulte Homes, Inc. v. Laborers' International Union of North America et al. Nos. 09-2245; 10-1673. 2 August 2011. 648 F.3d 295. Available at: https://www.opn.ca6.uscourts.gov/opinions.pdf/11a0200p-06.pdf.

11. United States Supreme Court. Burrage v. United States. No. 12-7515. 27 January 2014. 571 U.S. 204–219. Available at: https://www.govinfo.gov/content/pkg/USREPORTS-571/pdf/USREPORTS-571-204.pdf.

The article was submitted: *2026 September 17*
Accepted for publication: *2026 September 28*

Musayev E.♦

DOI: 10.25108/2304-1730-1749.iolr.2026.84.96-103
UOT: 343.3:004

Cinayət tərkibinin obyektiv əlamətləri və rəqəmsal mühitdə səbəbli əlaqə

Xülasə: Məqalədə rəqəmsal müdaxilə nəticəsində yaranan texniki dəyişikliklərin Azərbaycan cinayət hüququnda hansı şərtlərlə hüquqi əhəmiyyətli nəticə sayılması və davranışa aid edilməsi araşdırılır. Tədqiqatın məqsədi texniki hadisə, faktiki səbəbli əlaqə və hüquqi qiymətləndirmə arasındakı sərhədləri müəyyənləşdirməkdir. Araşdırma formal-hüquqi və doktrinal təhlili problem üzrə müqayisə ilə birləşdirir. Azərbaycan qanunvericiliyi və seçilmiş məhkəmə mövqeləri Almaniya və Amerika Birləşmiş Ştatlarının normativ, məhkəmə və elmi materialları ilə müqayisə olunur. Məqalədə xarici həllərin milli hüquqa avtomatik köçürülməsinə yol verilmir, statistik ümumiləşdirmə aparılmır, texniki nümunələr hipotetik model kimi istifadə edilir. Təhlil göstərir ki, verilənin dəyişməsi, sistemin fəaliyyətinə maneə, autentikliyin pozulması və əmlak itkisi fərqli hüquqi nəticələrdir. Qanunun ayrıca tələb etmədiyi zərər şərti tərkibə əlavə olunmamalı, tələb olunan nəticə isə təhlükə təsviri ilə əvəz edilməməlidir. Çoxsaylı müdaxilələrdə birlikdə yaranan nəticə, müstəqil kifayət edən səbəblər və səbəbkarın müəyyənləşdirilməsində sübut qeyri-müəyyənliyi fərqləndirilir. Təhlilin vahidi ayrı paketdən əvvəl sübutla şəxsə aid edilmiş davranış əsasında müəyyənləşdirilir. Nəticələrdən biri də odur ki, sistemin zəifliyi və üçüncü şəxsin sonrakı qərarı səbəbli əlaqəni avtomatik kəsmir. Hərəkətsizlikdə texniki imkan hüquqi hərəkət vəzifəsini əvəz etmir.Vəzifənin əsası və konkret nəticənin qarşısının alınması ayrıca yoxlanılır. Ekspertin texniki qənaəti cinayət tərkibinə uyğunluq və təqsir barədə hüquqi nəticənin yerini tutmur. Məqalədə fərdi davranış, faktiki mexanizm, alternativ səbəblər və hüquqi aidetmədən ibarət ardıcıl yoxlama təklif edilir. Yanaşmanın əhəmiyyəti rəqəmsal sübutların cavablandırdığı sualları dəqiqləşdirmək və məsuliyyətin qanuni hədlərini qorumaqdır. Təklif yeni ümumi cinayət tərkibi yaratmır və empirik təsdiqlənmiş model kimi təqdim edilmir. Qanunvericilik dəyişikliyindən əvvəl təfsir çətinliyi, sübut çatışmazlığı və həqiqi normativ boşluq ayrılmalı olduğu göstərilir.

Açar sözlər: qanunçuluq; verilənlərin bütövlüyü; xidmətin əlçatanlığı; çoxsəbəblilik; hərəkətsizlik; elektron sübut; ekspert rəyi; fərdi məsuliyyət.

Məqalə daxil olmuşdur: *17 sentyabr 2026-cı il*
Çapa qəbul edilmişdir: *28 sentyabrt 2026-cı il*

♦ **Musayev Erkin** - Bakı Dövlət Universiteti, Cinayət hüququ və kriminologiya kafedrasının doktorantı (Azərbaycan). E-poçt: musayev2022@gmail.com

Мусаев Э.♦

DOI: 10.25108/2304-1730-1749.iolr.2026.84.96-103
УДК: 343.3:004

Объективные признаки состава преступления и причинная связь в цифровой среде

Аннотация: В статье исследуются условия, при которых технические изменения, возникшие вследствие цифрового вмешательства, признаются юридически значимыми последствиями в уголовном праве Азербайджана и могут быть отнесены к определённому поведению. Цель исследования — установить границы между техническим событием, фактической причинной связью и правовой оценкой. Исследование сочетает формально-юридический и доктринальный анализ со сравнением по рассматриваемой проблеме. Законодательство Азербайджана и отдельные судебные позиции сопоставляются с нормативными, судебными и научными материалами Германии и Соединённых Штатов Америки. В статье не допускается автоматический перенос зарубежных решений в национальное право, не проводится статистическое обобщение, а технические примеры используются как гипотетические модели. Анализ показывает, что изменение данных, воспрепятствование работе системы, нарушение аутентичности и имущественная потеря представляют собой разные юридические последствия. В состав преступления не следует добавлять условие причинения вреда, которого закон отдельно не требует, а требуемое последствие нельзя заменять описанием опасности. При множественных вмешательствах разграничиваются совместно возникшее последствие, независимо достаточные причины и доказательственная неопределённость при установлении лица, причинившего последствие. Единица анализа определяется на основе поведения, отнесённого к лицу посредством доказательств, прежде чем рассматривать отдельный пакет. Один из выводов состоит в том, что уязвимость системы и последующее решение третьего лица не прерывают причинную связь автоматически. При бездействии техническая возможность не заменяет правовую обязанность действовать. Основание обязанности и предотвратимость конкретного последствия проверяются отдельно. Технический вывод эксперта не заменяет правового вывода о соответствии признакам состава преступления и о вине. В статье предлагается последовательная проверка индивидуального поведения, фактического механизма, альтернативных причин и юридического вменения. Значение подхода состоит в уточнении вопросов, на которые отвечают цифровые доказательства, и в сохранении законных пределов ответственности. Предложение не создаёт нового общего состава преступления и не представляется как эмпирически подтверждённая модель. Показано, что до изменения законодательства следует разграничивать трудности толкования, недостаточность доказательств и действительный пробел в законодательстве.

Ключевые слова: законность; целостность данных; доступность сервиса; множественность причин; бездействие; электронные доказательства; заключение эксперта; индивидуальная ответственность.

Дата поступления: *17 сентября 2026 г.*
Дата принятия в печать: *28 сентября 2026 г.*

♦ **Мусаев Эркин** - докторант кафедры уголовного права и криминологии Бакинского государственного университета (Азербайджан). Электронная почта: musayev2022@gmail.com