ISSN 2312-5160
online ISSN 2786-4502

Current Issues of Mass Communication, Issue 40 (2026)

*Journal homepage: https://cimc.knu.ua/index*

R E S E A R C H  A R T I C L E S
Д О С Л І Д Н И Ц Ь К І  С Т А Т Т І

https://doi.org/10.17721/CIMC.2026.40.33-53
UDC 351.751:004.738.5(477)

# From Prohibition to Overload: Data Closure, Digital Propaganda, and the Typology of Restrictions on Access to Information in Ukraine, 2022–2026

Yana Shekeriak-Kushka, Vladyslav Bilozerov
Ivan Franko National University of Lviv, Ukraine

**Objectives.** Digital platforms, artificial intelligence, and algorithmic systems increasingly shape informational reality, while demand for verifiable information grows. The article combines conceptual analysis with an empirical test. Its theoretical part examines the forms of digital control over information – direct censorship, digital propaganda, information overload, and the closure of public data and platform APIs – and proposes a common framework for describing them through four shared parameters – actor, formal basis, visibility, and affected link. Whether these forms share a common logic is treated here as an open question rather than an assumption, and is tested against documented material. The empirical part determines the parameters along which active restrictions, which add content, and passive ones, which withdraw it, differ and converge, and which links of the citizen's informational capacity each of them affects. **Method.** Structured documentary analysis of a corpus of 29 documented restriction events in Ukraine between 24 February 2022 and 5 September 2026, drawn from normative acts, monitoring reports, platform announcements, and specialized media. The unit of analysis is a single restriction event, coded on eight parameters; both authors coded the corpus independently, with intercoder agreement of $\kappa$ = .71–1.00 (M = .93). **Results.** Content removal does not occur as a primary type. Of the four parameters, only two vary independently: the actor predicts the formal basis in 24 of 27 events and visibility in 18, so basis and visibility behave largely as properties of the actor; concealed restrictions occur only among external actors. Most restrictions affect two links at once, production and verification. No state restriction was lifted in full. **Conclusions.** Active and passive restrictions converge in form but diverge in consequence: what differs is not the technique but the actor, the duration of the restriction, and whether a procedure for restoration exists. Artificial intelligence emerges not as a separate mechanism but as infrastructure that scales existing ones. Verification is affected in the great majority of cases in the corpus; data journalism, which rests on it, is vulnerable to the very restrictions it counters. Informational sovereignty – the citizen's ability to obtain, verify, and interpret data independently of state, platform, and media intermediaries – is proposed as a framework for studying freedom of speech, freedom of data, and the capacity for verification.

*Keywords*: data journalism, open data, media, digital propaganda, informational sovereignty, artificial intelligence, information overload, verification, censorship, content analysis, martial law, access to public information, Ukraine

**Citation**: Shekeriak-Kushka, Y., & Bilozerov, V. (2026). From prohibition to overload: Data closure, digital propaganda, and the typology of restrictions on access to information in Ukraine, 2022–2026. *Current Issues of Mass Communication*, *40*, 33–53. https://doi.org/10.17721/CIMC.2026.40.33-53

**Copyright**: © 2026 **Yana Shekeriak-Kushka, Vladyslav Bilozerov**. This is an open-access draft article distributed under the terms of the **Creative Commons Attribution License (CC BY 4.0)** https://creativecommons.org/licenses/by/4.0/. The use, distribution or reproduction in other forms is permitted, provided the original author(s) or licensor are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted if it does not comply with these terms.

ISSN 2312-5160
online ISSN 2786-4502

# Від заборони до перенасичення: закритість даних, цифрова пропаганда і типологія обмежень доступу до інформації в Україні, 2022–2026

Яна Шекеряк-Кушка, Владислав Білозеров
Львівський національний університет імені Івана Франка, Україна

***Цілі.*** Цифрові платформи, штучний інтелект і алгоритмічні системи дедалі більше формують інформаційну реальність, тоді як потреба у верифікованій інформації зростає. Стаття поєднує концептуальний аналіз і емпіричну перевірку. У теоретичній частині проаналізовано форми цифрового контролю інформації – пряму цензуру, цифрову пропаганду, інформаційне перенасичення та закритість публічних даних і платформних API – і запропоновано спільну рамку для їх опису через чотири спільні параметри – суб'єкт, формальна підстава, видимість, уражена ланка. Чи мають ці форми спільну логіку, тут потрактовано як відкрите питання, а не як припущення, і перевірено на задокументованому матеріалі. Емпірична частина визначає параметри, за якими розрізняються й збігаються активні обмеження, що додають контент, і пасивні, що його вилучають, та які ланки інформаційної спроможності громадянина уражає кожне з них. ***Метод.*** Структурований документальний аналіз корпусу з 29 задокументованих подій обмеження в Україні від 24 лютого 2022 року до 5 вересня 2026 року за нормативними актами, моніторинговими звітами, повідомленнями платформ і публікаціями спеціалізованих медіа. Одиниця аналізу – окрема подія обмеження, закодована за вісьмома параметрами; обидва автори закодували корпус незалежно, міжкодувальна узгодженість κ = 0,71–1,00 (M = 0,93). ***Результати.*** Видалення контенту як основний тип не трапляється. З чотирьох параметрів лише два варіюються незалежно: суб'єкт передбачає формальну підставу у 24 випадках із 27 і видимість у 18, тож підстава й видимість поводяться радше як властивості суб'єкта; приховані обмеження є лише в діях зовнішніх акторів. Більшість обмежень уражає дві ланки одночасно – виробництво й верифікацію. Жодне державне обмеження не було скасоване повністю. ***Висновки.*** Активні й пасивні обмеження збігаються за формою, але розходяться за наслідками: різниця не в техніці, а в тому, хто обмежує, як довго триває обмеження і чи існує процедура відновлення. Штучний інтелект постає не окремим механізмом, а інфраструктурою, що масштабує вже наявні. Верифікацію уражено в переважній більшості випадків корпусу; журналістика даних, яка на ній тримається, вразлива до тих самих обмежень, яким протидіє. Інформаційний суверенітет – здатність громадянина отримувати, перевіряти й інтерпретувати дані незалежно від державних, платформних і медійних посередників – запропоновано як рамку для дослідження свободи слова, свободи даних і спроможності до верифікації.

*Ключові слова*: журналістика даних, відкриті дані, медіа, цифрова пропаганда, інформаційний суверенітет, штучний інтелект, інформаційне перенасичення, верифікація, цензура, контент-аналіз, воєнний стан, доступ до публічної інформації, Україна

Freedom of information has traditionally been conceptualized through the lens of censorship – as a visible, institutionally formalized act of prohibition. However, the digital environment has produced fundamentally different forms of restricting access to knowledge, which operate not through silencing but through excess, not through closure but through opacity. The contemporary citizen finds themselves caught between two simultaneous threats: a stream of unverified content that saturates the media space, and the systematic inaccessibility of public data on which they could form an independent judgment.

Russia's full-scale invasion of Ukraine in 2022 exposed these vulnerabilities with particular acuteness: information warfare and data closure turned out to be two sides of the same

Yana Shekeriak-Kushka https://orcid.org/0000-0002-8187-4062
Vladyslav Bilozerov https://orcid.org/0009-0004-4556-8916
Yana Shekeriak-Kushka is an assistant professor in the New Media Department. Her research interests include data journalism, infographics, the gamification of journalism, media technologies, propaganda, and fake news. Vladyslav Bilozerov is an assistant professor and a PhD student (New Media Department). His research interests include propaganda, social networks, new media, AI, media philosophy, mass communication, and storytelling. Correspondence concerning this article should be addressed to: Yana Shekeriak-Kushka, shekeriakya@gmail.com

ISSN 2312-5160
online ISSN 2786-4502

phenomenon. Research on the dissemination of official information under wartime conditions demonstrates that existing regulatory frameworks contain significant gaps in ensuring timely and reliable access for citizens to public data – and that these gaps directly undermine societal resilience and trust in institutions (Oleksiyuk, 2025).

This article brings together two kinds of restriction that are usually analyzed apart – the active production of content and the passive withdrawal of data – and asks whether they operate as complementary mechanisms of a single system of control over knowledge.

## Literature Review

Research on propaganda and disinformation in the digital environment has a long tradition. Benkler et al., in their foundational work Network Propaganda (2018), show that disinformation campaigns operate not as isolated operations but as systemic phenomena embedded in the media ecosystem. Subsequent research in the context of the Russian-Ukrainian war treats digital communication not only as a channel through which the war is reported but as an instrument within it (Jungblut et al., 2023), and has shown that citizens across nineteen countries differ in whether they read false information as error or as intent (Hameleers et al., 2024).

According to Ni et al. (2023), information overload can be used to alienate different media users not only in democratic countries but also in authoritarian regimes with strong unified ideologies. Nor is this strategy limited to creating news avoidance. Jasser (2023) identified and modeled a situation in which an information-saturated social media field was used for a disinformation campaign. Bermes (2021) reached a similar conclusion while studying the media field during the COVID-19 pandemic and found that information overload makes users more susceptible to consuming and spreading disinformation. Furthermore, Szegőfi et al. (2026) found that an environment with disinformation overflow can even alter the opinions of users who previously had strong positive beliefs on the topic.

In parallel, the field of data journalism and open data research developed. Camaj et al. (2025) and Martin et al. (2024) established that unequal access to public information infrastructure directly determines the quality of data journalism: in countries with limited transparency, journalists are systematically forced to circumvent institutional obstacles instead of obtaining data through normal public access. Researchers from Greece and Denmark (Papageorgiou et al., 2023), in a conference paper presenting a domain mapping review of publications on open data journalism for 2010–2022, concluded that the availability of public data is not an additional advantage but a structural precondition for accountable journalistic coverage of government activity.

At the same time, research on information overload shows that an excess of information is not merely a side effect of the digital environment but also a controllable instrument. Where information is abundant and attention is not, what spreads is selected for consistency with existing belief rather than for accuracy, so that an excess of available information can leave a reader with a more polarized picture than a scarcity of it would (Hills, 2019). This closes a loop in which both censorship and excess serve the same purpose – to make verification impossible.

The closure of platform APIs has become a new form of structural restriction: X (Twitter) announced the end of free API access in February 2023 and introduced a new pricing structure in March, leaving no academic tier, and Meta closed CrowdTangle in August 2024, having announced the closure five months earlier – thereby depriving independent researchers and journalists of data access that had existed for years (Casas et al., 2025). This means that even where openness existed, it remained a privilege rather than a right.

Grübl et al. (2026) review modern internet censorship infrastructure and propose a framework for further study. However, they pay little attention to information overload, probably because this instrument of digital disinformation is difficult to frame and measure.

ISSN 2312-5160
online ISSN 2786-4502

This is symptomatic of a wider pattern we observe across the literature: research on digital propaganda and research on open data have developed largely apart, each treating the restrictions it studies as different in kind from those studied by the other, and the question of whether they share a common logic has not been tested against documented material.

*Active and Passive Restriction of Access to Information*

Today it may seem that any information on the internet is available to anyone with the technical means to connect to the network. This illusion was born in the era of the early internet, when both scholars and the general public believed it would become an instrument of global integration and the pinnacle of freedom of information. In part, the internet did develop this way, as points of entry (computers and mobile phones) became accessible to an ever-growing number of users. However, the question of controlling information flows was too important for many states simply to turn a blind eye to it.

Direct censorship has long been used: information disliked, for any reason, by the principal administrator of the information space is simply removed. When such an administrator disappeared with the transition to the internet, the search for new methods of control began. But conventional censorship kept pace as well. States began blocking access either to the entire global network (for example, China or North Korea), creating their own analogues, or only to individual sites that published information undesirable to them.

Social networks developed as an information space within an information space, creating large-scale echo chambers inside the global network. One of the main unifying factors of any social network is a set of rules and the user's compliance with them: the uncontrolled information flow, which in the era of the early internet was restricted only in the case of criminal content, came to be governed not merely by a country's legislation but by the policy of the owner company. Industry giants such as Meta and ByteDance apply their own policy on desirable and undesirable content alongside legal compliance, including rudimentary non-contextual algorithmic censorship that removes or blocks messages containing certain keywords or images without human intervention. The rules themselves are published; how they are enforced is not – ranking, recommendation, and demotion thresholds remain undisclosed, so a user can rarely establish whether a given piece of content was restricted at all. What emerges is not a transfer of control to corporations but a division of it: states set the outer legal limits, while corporations decide what circulates within them, accountable to users and to host countries only to a limited degree.

Ordinary censorship is fairly easy to recognize: information about removal is available and is often displayed as notices about banned profiles, deleted posts, or court decisions. The digital era, and especially the development of artificial intelligence, has strengthened the capacity to control information flows through instruments that are not recognizable in this way – contextual censorship and information noise.

Contextual censorship has become an important factor specifically in the realm of social networks, since information about the user is easier to collect there. It works like any contextual mechanism: it assesses the user's previous activity and the tendencies of the surrounding information environment and, on this basis, determines what to show and what not to. Feeds in most social networks work this way – Facebook and Instagram, TikTok, X, YouTube recommendations, and Google search alike. The user is thereby driven, without their knowledge, into an echo chamber that makes access to other information difficult, fragmenting the information space and intensifying radicalization in closed communities. The threat lies in the opacity of selection: companies do not disclose how users are assessed or which data are taken into account, and control over information flows remains with profit-focused corporations.

The term "information pollution" dates to the 1970s (Ettinger, 1971), but the condition it names became consequential later, as the volume of information available online grew through the

ISSN 2312-5160
online ISSN 2786-4502

2000s – large enough for propaganda and bad-faith actors to turn excess itself into an instrument, information noise. One of the most striking examples of its use is Russian propaganda when it needs to conceal its crimes. The downing of the Malaysia Airlines Flight MH17 in 2014, the destruction of the Mariupol Drama Theatre and the maternity hospital, the shelling of Kramatorsk railway station, the destruction of the Kakhovka Hydroelectric Power Plant – these are only some of the most indicative cases in which, within a matter of hours, several incompatible versions of the same tragedy were circulated at once, blurring the information reality and reducing the ordinary user's willingness to seek objective information. Accordingly, the genuine and objective message is lost amid this stream. In the coded corpus, this practice appears as information noise (3 events; see Table 1).

If censorship and propaganda operate through active production and suppression, the closure of public data is a passive but no less effective mechanism of restriction. Where there is no access to registries, official statistics, or machine-readable formats of state reporting, the citizen and the journalist are deprived of the tools of independent verification – even if formally no one prohibits anything.

The study by Camaj et al. (2025) demonstrates that unequal public policies regarding governmental transparency directly determine the quality and possibilities of data journalism: in countries with limited transparency infrastructure, journalists are systematically deprived of the tools for accountable coverage of those in power. The closure of registries, the absence of machine-readable formats, or formal openness without real accessibility – this is not a technical problem but a political choice.

Data journalists develop strategies for circumventing these restrictions. However, research shows that they are systematically forced to "scrape, request, collect, repeat" – that is, to overcome institutional obstacles instead of obtaining data through normal public access (Martin et al., 2024). This shifts the systemic responsibility of the state onto individual journalists and newsrooms, making accountable journalism dependent on the resources of specific newsrooms.

Importantly, active restriction through the production of content and passive restriction through the withdrawal of data may converge on the same ultimate effect: the citizen cannot verify reality. If so, they differ in how this effect is produced, not in what it produces: one fills the space with the false, the other removes the tools for verifying the true. Whether this holds is an empirical question. Answering it requires describing both forms in the same terms. We propose four parameters that apply to active and passive restriction alike: the actor who restricts, the formal basis invoked, the visibility of the restriction to the user, and the link of informational capacity it affects. These parameters form the framework of this study and are operationalized in the coding scheme set out below, together with further parameters describing the type, character, and duration of the restriction.

The article has two aims. The first is conceptual: to propose a common framework for describing active and passive restrictions on access to information through a shared set of parameters. The second is empirical: to determine the parameters along which they differ and converge, and which links of the citizen's informational capacity each of them affects.

## Method

### Design

This is an empirical study based on structured documentary analysis. The unit of analysis is a single restriction event: a documented decision or action after which access to specific data or content became unavailable, incomplete, or conditional. Events are coded according to a fixed scheme. The notion of informational sovereignty is retained not as a method but as the interpretive framework within which results are read.

ISSN 2312-5160
online ISSN 2786-4502

## Definitions

Two terms used throughout require explicit definition. Mechanism is understood here as a recurring configuration of coded parameters – actor, formal basis, visibility, and affected link – that appears repeatedly across the corpus. Whether a given practice constitutes a mechanism in this sense is therefore an empirical question answered in the Results, not a claim asserted in advance. Informational sovereignty denotes the capacity of the citizen, not of the state. This distinction is stated explicitly because in Ukrainian legal usage the term is conventionally applied to the state. Here it means the citizen's ability to obtain, verify, and interpret data independently of state, platform, and media intermediaries. Each of these forms of mediation is increasingly enacted through algorithmic and AI-based systems.

## Material

The corpus comprises 29 documented restriction events in Ukraine between 24 February 2022 and 5 September 2026 (the corpus closing date, on which all acts were verified); the most recent event included dates to January 2026. Sources are of four types: normative acts and administrative decisions; monitoring reports by professional organizations; official platform announcements; and publications by specialized media documenting cases of denied access. Inclusion criteria: the event is dated within the period; attested by at least one primary or authoritative secondary source; concerns data or content relevant to journalistic verification; and the onset of the restriction can be established. Two events were subsequently excluded as falling outside the object of study, leaving 27 coded events. The full list of coded cases is given in Appendix B (Tables B1 and B2).

The corpus covers practices of restricting access, so events that expand access do not enter it. Such events did occur: Cabinet of Ministers Resolution No. 236 of May 2023 narrowed the grounds for suspending or limiting the operation of information systems and public electronic registries to front-line and temporarily occupied territories, removing the legal basis on which rear cities had kept their portals closed. The direction of movement over the period was not uniformly toward closure. Public access to asset declarations returned in December 2023 after a legislative change, the company register was reopened in January 2026 with some fields removed, and the number of datasets listed on the national portal recovered from its 2023 low to within a tenth of the pre-invasion figure. This is noted so that the asymmetry of the corpus is not read as bias in sampling.

## Coding scheme

Each event was coded on eight principal parameters: type of restriction, character of restriction, actor, formal basis, visibility to the user, reversibility, affected link of informational capacity (three independent binary variables), and duration. The character variable distinguishes direct restriction (the act prescribes terminating or removing access) from indirect restriction (the act alters a procedure, as a result of which data cease to be produced or lose completeness, with no prescription regarding access), alongside mixed cases and cases where the variable does not apply. Two further variables replace evaluative judgment with fact: whether a security justification was publicly declared, and whether named professional organizations contested the restriction. The security-justification variable records whether the act names what is being protected. A reference to martial law as a circumstance is not counted, since it appears in the preamble of most acts of the period and therefore does not differentiate cases; a named object of protection is counted, as when the National Agency on Corruption Prevention cited the personal data of declarants, the State Judicial Administration of Ukraine cited the life and health of judges, and the Ministry of Justice cited the protection of information. Proportionality is not assessed.

ISSN 2312-5160
online ISSN 2786-4502

**Dating rule**

The event is the restriction, not its disclosure. The date of public disclosure is coded separately. The interval between onset and disclosure is a measurable quantity and serves as the empirical basis for the visibility variable.

**Comparative cases**

Three non-Ukrainian cases (Russia, the United States, India) were coded with the same instrument but are reported separately and excluded from the quantitative distributions. Each tests a specific alternative explanation of the findings.

**Procedure and coding reliability**

Coding proceeded in three stages: pilot coding on a subset of the corpus; refinement of the codebook in response to boundary cases identified during the pilot; and independent double coding of the full corpus by both authors working separately. Intercoder agreement was assessed using Cohen's κ for each categorical variable, computed in Python (scikit-learn) with the assistance of an AI tool from the two independently coded files. Agreement ranged from substantial to almost perfect (κ = .71–1.00, M = .93); six variables reached complete agreement. Of the nine disagreements recorded, two proved to be data-entry errors; the remainder were resolved through discussion, one of them prompting an explicit boundary rule in the codebook. The full coding workbook, containing the codebook, case list, coded data, and reliability log, is openly available (Shekeriak-Kushka & Bilozerov, 2026).

**Limitations of the method**

The corpus is not exhaustive: only documented cases are coded, so covert restrictions are not represented. Events that expanded access were not coded, so the corpus supports no statement about the balance between restriction and restoration over the period. Several spheres were checked without result, and the municipal level was not coded, since restrictions there consist of hundreds of separate decisions with no common act or date. Ukrainian events are documented predominantly in media rather than normative sources, so formal bases are less often available for state actions than for platform actions. State actions are confined to a single jurisdiction whereas platform actions are transnational, which complicates direct comparison. For two procurement-related events, amendments introduced by Cabinet of Ministers Resolution No. 957 of 15 July 2026 took effect on 1 September 2026, four days before the corpus closed, and their full bearing on the coded provisions could not be assessed.

**Four features of the scheme itself set further limits**

The formal-basis variable records whether an actor named a basis, not whether that basis was sufficient; no variable assesses the relevance of the cited provision, as this is a legal interpretation the authors do not undertake. The affected-link variables record the coders' assessment of which link a restriction reaches, not a measured magnitude of effect. Verification in particular is affected in almost every event, but this is in part built into the sampling: relevance to journalistic verification is an inclusion criterion, so the corpus shows how restrictions that bear on verification are otherwise configured, not how often restrictions in general bear on it. Depth of consequence is therefore approached indirectly, through duration and reversibility, which are recorded as facts about the act rather than as judgments about its effects. Second-order effects are not coded: the increased cost of gathering material in a saturated information space is not counted as an effect on production, which chiefly concerns external-actor campaigns, where the production variable takes

ISSN 2312-5160
online ISSN 2786-4502

the value "no" despite a real effect on newsroom work. For the Russian comparative case no Russian sources were used, and contestation is coded as "no data" irrespective of any actual reaction within that jurisdiction, since public contestation of state decisions there carries legal consequences; comparison on this variable across jurisdictions with different legal regimes is therefore limited. Finally, twenty-seven coded events support descriptive analysis: the distributions and cross-tabulations illustrate configurations of features rather than demonstrating statistical dependencies. The event-based model of restriction on which this study is built captures decisions about access but does not capture restrictions that arise without an event and without an actor – a limit addressed in the Discussion.

## Results

Twenty-seven events were coded. The number of observations varies across variables: events with the status “attempted, not enacted” are coded on a reduced set of variables, so N = 26 for type of restriction, reversibility, duration, and security justification, and N = 27 for the remaining variables. Distributions by actor, formal basis, and visibility, together with further distributions and cross-tabulations, are given in Appendix A.

### Types of Restriction and Actors

**Table 1.** ***Distribution by Type of Restriction (N = 26)***

| Type of restriction | n | % |
|---|---|---|
| registry closure | 7 | 26.9 |
| narrowing of data scope | 7 | 26.9 |
| access blocking | 4 | 15.4 |
| API termination | 3 | 11.5 |
| information noise (flooding) | 3 | 11.5 |
| algorithmic downranking | 1 | 3.8 |
| deferral of publication | 1 | 3.8 |
| content removal | 0 | 0.0 |

Two types dominate in equal proportions: registry closure and narrowing of data scope together account for more than half the corpus. The zero value deserves separate attention: content removal – the mechanism conventionally identified with censorship – does not occur as a primary type in the corpus (it appears once as a secondary type; see Appendix A). Restriction of access to information in Ukraine during the period studied operated not through withdrawing what had been published, but through terminating or narrowing publication itself.

The typology also has a visible limit. All three external-actor campaigns (R023, R024, R025) receive the same code, information noise, although they operate through three distinct mechanisms: substitution of a trusted source by cloning specific outlets; mass retransmission through hundreds of aggregators; and impersonation of individuals and institutions combined with overloading fact-checkers. A typology built on actions taken with respect to access does not differentiate these campaigns, because they do not restrict access at all – they substitute or saturate content. This is evidence that active and passive restrictions differ in kind, and to that extent the data work against the initial expectation of convergence between them.

The state is the most frequent actor of restriction (16 events; 59.3%), followed by platforms (7; 25.9%) and external actors (4; 14.8%). Restrictions rest on statutory grounds in 13 cases (48.1%), on platform policy in 7 (25.9%), and on no stated formal basis in 7 (25.9%). Visibility is

ISSN 2312-5160
online ISSN 2786-4502

evenly split between explicit and discoverable (12 each; 44.4%), with 3 concealed cases (11.1%); the full distribution is given in Appendix A, Table A1.

**Actor and Visibility of Restriction**

**Table 2.** ***Actor × Visibility (N = 27)***

| Actor | explicit | discoverable | concealed | Total |
|---|---|---|---|---|
| state | 6 | 10 | 0 | 16 |
| platform | 5 | 2 | 0 | 7 |
| external actor | 1 | 0 | 3 | 4 |

As shown in Table 2, visibility is strongly structured by the actor, though not determined by it. Concealed visibility occurs exclusively in the actions of external actors, in three of their four cases, and in no state or platform case. Within the state and platform categories, however, both explicit and discoverable restrictions occur, so knowing the actor narrows the expected visibility without fixing it.

**Table 3.** ***Actor × Formal Basis (N = 27)***

| Actor | law | platform policy | no basis stated | Total |
|---|---|---|---|---|
| state | 13 | 0 | 3 | 16 |
| platform | 0 | 7 | 0 | 7 |
| external actor | 0 | 0 | 4 | 4 |

The distribution by formal basis is more unequivocal still (Table 3): every platform restriction rests on platform policy, every external-actor restriction states no basis, and state restrictions overwhelmingly rest on statutory grounds. No overlap between basis categories across actor types was recorded.

Taken together, Tables 2 and 3 qualify the proposed framework rather than confirm it. The four parameters do not vary independently. Knowing the actor predicts the formal basis in 24 of the 27 events and the visibility of the restriction in 18. Basis is the more strongly determined of the two: the only state restrictions that name no basis are the three enacted on 24 February 2022, the first day of the invasion, and every state act after that date cites a statutory ground. Of the four parameters, then, two carry information of their own – the actor and the affected link – while basis and visibility behave largely as properties of the actor rather than as dimensions along which actors can be compared. This is a finding about how restriction is organized, and not one the framework anticipated: each type of actor restricts in its own way and declares it in its own way, and the two cannot be varied separately.

The basis variable records whether an actor named a basis, not whether the provision cited actually governs access. In several state cases the two diverge: the act names a statutory ground, but the provision invoked contains no prescription regarding access to the data in question. This study does not undertake that legal assessment; the qualification is drawn from the monitoring work of professional organizations, which recorded the absence of a three-part test in the acts concerned.

One of the three state restrictions with no stated basis shows what "no basis stated" can conceal. The national open data portal was shut down in February 2022 and restored in August; on the day of restoration the Ministry of Digital Transformation announced a public consultation on legislative amendments intended to establish rules of access to open data under martial law. The

ISSN 2312-5160
online ISSN 2786-4502

regulatory basis was thus being drafted after the restriction had been in force for more than five months. This is not a case of an unstated basis but of a basis that did not exist at the time of the restriction. The scale of the withdrawal at this portal can be read from archived copies of its catalog: 40,989 datasets were listed on 23 February 2022, the day before the invasion, and 28,764 on 14 March 2023 (Ministry of Digital Transformation of Ukraine, 2022, 2023). The count then recovered over the following three years, to 39,800 on 11 February 2026, and stood at 36,930 in October 2026 (Ministry of Digital Transformation of Ukraine, 2026a, 2026b). Recovery of the count is not recovery of the data, however: as the reversibility coding below shows, datasets returned with fields removed or with a category replaced, so the figure says how many entries the catalog holds and not what they contain. These counts describe one portal, are not part of the coded corpus, and are given to indicate the order of magnitude involved.

The interval between the onset of a restriction and its disclosure was calculated for the 21 events dated to the day (Table 4).

**Table 4.** ***Disclosure Regime (N = 21)***

| Regime | n | % | Actors |
|---|---|---|---|
| announced in advance | 6 | 28.6 | state 3, platform 3 |
| simultaneous (0 days) | 12 | 57.1 | state 8, platform 3, external actor 1 |
| discovered after the fact | 3 | 14.3 | state 3 |

The median lead time in the advance-announcement regime is 48 days. Intervals in the after-the-fact regime are 6, 72, and 158 days. Notably, all three cases in which a restriction became known only after it had taken effect are state administrative decisions; no such case was recorded for platforms or external actors.

### Affected Links of Informational Capacity

Restrictions affect the three links in four combinations: production and verification together (20 events; 74.1%), perception alone (3; 11.1%), perception with verification (2; 7.4%), and all three (2; 7.4%); see Appendix A, Table A4. Taken separately, production is affected in 22 events (81.5%), verification in 24 (88.9%), and perception in 7 (25.9%). The overwhelming majority of restrictions (81.5%) affect exactly two links, and almost always the same pair – production and verification.

This finding refines the initial assumption that censorship restricts production, overload restricts perception, and data closure restricts verification. The data show that these links are not distributed across mechanisms: a single event typically affects production and verification simultaneously. Perception, by contrast, is affected separately and barely overlaps with the rest – in two of the four combinations it appears without production being affected.

### Reversibility of Restrictions

More than half of all restrictions (15 of 26; 57.7%) had not been lifted as of the corpus closing date. The principal pattern: no state restriction was fully lifted – access was either partially restored (7 cases) or not restored at all (8). All three cases of full restoration involve platforms and an external actor; see Appendix A, Table A5. Restoration of access is not equivalent to restoration of data: in several cases access returned while the dataset did not, either with fields removed or with a category replaced, so analysis by the previous methodology is no longer possible.

ISSN 2312-5160
online ISSN 2786-4502

Two events allow a closer comparison, since they share a type but differ in actor. In R002 a state registry was closed by the state's own decision; in R026 the same kind of access was lost to an external cyberattack. Both are coded as registry closure, both affect production and verification, and both concern comparable data. The outcomes diverge sharply. The state closure lasted more than three years, restoration was partial, the act named no basis, and a justification followed four months later. The cyberattack lasted 32 days, restoration was complete, and disclosure came the same day. The mechanisms are comparable in form; the consequences for a citizen's capacity to verify are not. What differs is not the technique of restriction but who restricts and whether a procedure for restoration exists. This refines rather than refutes the initial expectation that active and passive restrictions converge: they converge in form and diverge in depth of effect.

The hypothesis that contestation by professional organizations promotes the restoration of access finds little support in this material: of the 17 contested restrictions for which reversibility is coded, 10 were not lifted, 6 were lifted partially, and 1 was lifted in full. Contestation does not distinguish restored from unrestored cases here, although the one case of full restoration is also a contested one, and with numbers this small the absence of a pattern is not evidence that contestation is without effect.

That one case runs the other way and is worth stating, since it is also the only instance of algorithmic downranking in the corpus. In February 2024 Meta made reduced recommendation of political content the default on Instagram and Threads, rolling it out the following month. Accountable Tech tracked five accounts with more than 10,000 followers each that regularly posted political content over the eleven weeks from 8 March to 24 May 2024 and recorded an average weekly decline of 6.5% in reach per post, which the report projects as a fall of 65% across the period – one of the few restrictions in the corpus with any measured effect, and a projection from a trend line rather than a before-and-after comparison (Accountable Tech, 2024a). An open letter published on 10 April 2024 was signed by more than 200 creators with a combined following of more than 18 million, asking that the setting be opt-in rather than default (Accountable Tech, 2024b). The restriction was reversed in January 2025. In announcing the reversal, the head of Instagram stated that it had "proven impractical to draw a red line around what is and is not political content" (Mosseri, as cited in Washenko, 2025) – a statement from the restricting party itself about the opacity of its own criteria.

Restrictions were ongoing at the corpus closing date in 16 cases (61.5%) and had lasted more than a year in a further 6 (23.1%). Security justifications are declared exclusively by state actors: all 11 cases of declared justification (including three declared post hoc) are state actions, whereas no platform restriction and no external-actor restriction carries a justification. Indirect restrictions constitute a negligible share (1 case; 3.7%), so the principal indicators were not calculated separately for direct and indirect cases. Full distributions by character, duration, security justification, and contestation, as well as the cross-tabulation of restriction type by reversibility, are given in Appendix A, Tables A2 and A3. The single indirect case is independently described in the European Commission's 2024 report on Ukraine, which notes that data collection by the State Statistics Service is very limited because respondents are not obliged to provide data under martial law (European Commission, 2024, p. 11).

## Comparative Cases

Three non-Ukrainian cases were coded with the same instrument and placed outside the quantitative counts. Each tests a distinct alternative explanation of the findings. The suspension of foreign-trade statistics in Russia (2022) tests whether data closure is specific to Ukraine’s situation. The removal of federal datasets and web pages in the United States (2025) tests whether armed conflict is a necessary condition for such restrictions. The mobile internet shutdown in Punjab, India (2023) tests whether this set of practices is confined to a particular type of political regime.

ISSN 2312-5160
online ISSN 2786-4502

None of the alternative explanations was supported: all three cases reproduce mechanisms recorded in the main corpus, including outside a wartime context and outside a single jurisdiction. In the United States case a federal court subsequently found that the data had been withdrawn without adequate notice or reasoned explanation – an external confirmation that the visibility variable captures an observable property of the act rather than a judgment of the coders (Doctors for America v. Office of Personnel Management, 2025).

## Discussion

### AI as Infrastructure for Scaling Restriction

Estimates of how much of the web is now machine-written should be read with care. A study of 43,000 randomly sampled English-language articles published between 2020 and 2025 found that the share classified as AI-generated passed the share classified as human-written in late 2024 and then leveled off; the classification rests on a single detector, with a measured false-positive rate of 4.2% and a false-negative rate of 0.6% on texts known to be machine-generated, and a later version of the same study, averaging three detectors, puts the share about three percentage points lower (Graphite, 2025). The share itself is not the threat – users took up a new tool available to them. What matters for access to information is a narrower case: content produced in volume not to be read but to occupy the space where reading happens. The Pravda network (R024) in this corpus is exactly that – roughly 3.6 million articles in 2024 across 150 domains in dozens of languages (American Sunlight Project, 2025) – and its measurable effect falls on machines rather than on readers: an audit of ten chatbots found that 33% of their responses on the network's themes reproduced its claims (Sadeghi & Blachez, 2025).

Scale is the core instrument of disinformation: no campaign succeeds without a large volume of messages focused on different target-audience groups. Until recently, this meant either people who, for a low price, created and disseminated the messages the client wanted, or algorithms that responded to keywords and disseminated uniform messages. The ceiling of both was the same – an inability to adapt and the enormous resources required for contextualization.

Then large language models emerged, able to conduct near-human conversations online and to perceive everything said through the lens of a large context. This made it possible to cut the cost of running bots: instead of hiring hundreds of people, only a few are now needed to handle the narrative and technical support of a campaign across several thousand accounts. It also became possible to automatically generate articles of varying length in order to spread the narratives desired by bad-faith actors and to reinforce their theses with pseudo-substantiated analytics. Thanks to its ability to process large arrays of data, AI can also analyze a campaign’s course while it runs, assess its effectiveness, find patterns, and make corrections to improve dissemination. All this content is unique enough that the ordinary user cannot, at a quick glance, identify the campaign that produced it.

In addition, deepfake technology, based on neural networks, is a serious threat to the information field (Sanderson et al., 2024). But the threat is not so obvious. Deepfake videos of public figures are fairly easy to recognize due to the imperfection of the algorithms. Audio deepfakes are harder to recognize due to the absence of visual generation artifacts, but the insufficient amount of training material produces odd stress patterns and uncharacteristic constructions. And there remains one more not-so-obvious threat, namely the so-called "liar's dividend" (Chesney & Citron, 2018): a bad-faith actor can simply claim that a video or audio in which they do or say something damaging to them is a deepfake. In this way, trust in visual and audio materials is destroyed even when they are genuine.

The threat to the data field is of a different nature: generative models are capable of producing statistically plausible but fabricated datasets, as well as manipulative visualizations that preserve

ISSN 2312-5160
online ISSN 2786-4502

the outward appearance of objectivity. This is a new type of manipulation – not through lies but through the imitation of evidentiary force.

In addition, AI intensifies the problem of information overload, which is itself a mechanism of restricting verification. Research shows that under conditions of abundance the information that spreads is selected for consistency with prior belief rather than for accuracy (Hills, 2019). When there is too much data and it contradicts itself, the reader loses the ability to verify, regardless of whether they are an ordinary citizen or a professionally competent journalist. What generative models change is the supply side of this process: the selection pressure operates on whatever volume of content is available, and that volume is no longer bounded by the cost of writing it.

According to Zheng and Zhan (2026), data access restrictions affect not only human users but also AI systems. Hiding high-quality research and academic papers behind paywalls pushes AI to consume only free-access material, creating a closed loop of self-generated synthetic data circulating in AI systems. The two types of restrictions intersect at this juncture: peer-reviewed work is excluded from free access, while networks built in order to be ingested are still available. R024 is intentionally designed to be disseminated, without a paywall or registration process, and it spans 150 domains of machine-readable text. Consequently, closure and saturation operate on the same training corpus in opposing directions.

**Data Journalism as a Tool of Counteraction and New Vulnerabilities**

In the normative theory of the press, journalism is viewed as an institution of control over power (the "fourth estate"). The use of data allows journalists to back up their publications with verified evidence (Papageorgiou et al., 2023). Where registries are open and accessible, journalists can verify – and thereby counter both propaganda and disinformation. This is the systemic response of data journalism to both forms of restriction.

However, under conditions of armed conflict, data journalism itself becomes a target. Since the beginning of the full-scale invasion, cyberattacks against media, unlawful surveillance of investigative journalists, and restrictions on access to information have been recorded in Ukraine (Freedom House, 2024). The closure of registries for security purposes is an understandable mechanism for protecting military and state secrets. In parallel, however, the electronic asset declarations of politicians were also closed and were reopened only after media and public pressure.

Another vulnerability is the audience's distrust of complex content. Even where data journalism functions and data are available, the audience may not accept evidence-based content – especially under conditions of prolonged information overload, which forms a habit of consuming short and straightforward messages. The coded corpus does not support a neat division of labor between these forms. Restrictions do not each target a separate link: in 20 of 27 events (74.1%) a single restriction affected production and verification simultaneously, while perception was affected largely separately (7 events; 25.9%). What the corpus shows is not three parallel processes with distinct targets, but a recurring pair – production and verification – reached by different means. Platform dynamics compound this: the verification function of data journalism remains systemically dependent on the decisions of corporations accountable neither to readers nor to society.

The world's leading newsrooms – The Guardian, The New York Times, Reuters – have long opened their own schools of data journalism and verification. In Ukraine, data journalism is taught at a number of universities, at both bachelor's and master's levels – among them Taras Shevchenko National University of Kyiv, Odesa Polytechnic National University, and the National University of Kyiv-Mohyla Academy – and through initiatives such as KSE Media Lab and Texty.org.ua; the examples named here are illustrative rather than exhaustive. Integration nonetheless remains partial: most courses exist as separate disciplines rather than as a cross-cutting competency.

The response to systemic vulnerabilities lies not only in technical or regulatory solutions but also in educational ones. Media literacy and data literacy – that is, the ability to critically read,

evaluate, and verify data – are becoming basic competencies of the citizen of the digital age. This is especially relevant in the context of training future journalists and communication professionals: an understanding of the mechanisms of data manipulation, the principles of how algorithms work, and the logic of open registries must be integrated into educational programs rather than remaining an optional skill for the "technically savvy."

Techniques of misleading visualization long predate AI. What generative models change is the cost of producing them. Pseudo-scientific analytics, backed by convincing infographics and fictitious references, becomes practically impossible to distinguish from genuine work under conditions of information overload.

An important instrument of counteraction is also the development of a culture of verification at the level of media consumption. Research shows that even brief "inoculation" interventions – in the cited study, a game in which players practice the techniques by which misleading content is made, among them impersonating a trusted source and discrediting an opponent – measurably increase resistance to disinformation (Roozenbeek & van der Linden, 2019). The techniques specific to data – a truncated axis, an unstated denominator, a chart whose source is not given – would be the natural extension of this approach, bringing data literacy within the same inoculation logic. This means that data literacy can be not only a university discipline but also a practice of public communication: infographics with an explanation of methodology, open datasets accompanying materials, "why we use precisely this data" – all of this forms an audience capable of evaluating evidentiary force rather than merely consuming conclusions.

The concept of "freedom of speech" proves insufficient to describe this condition: one can have the formal right to speak – and not have access to the data on the basis of which this speaking could be reliable. This is precisely why we propose the concept of informational sovereignty – as the citizen's ability not merely to receive information but to verify it independently of the state, platforms, and media intermediaries. This concept unites freedom of speech and freedom of data into a single problem – and demands a single response at the level of regulation, journalistic practice, and media education.

One element of the concept is already measurable. The interval between the onset of a restriction and its public disclosure, recorded in days, provides an empirical basis for visibility: in this corpus it ranges from 153 days of advance notice to 158 days of delayed discovery, and its sign distinguishes platform and legislative action from state administrative decisions. Fuller operationalization of informational sovereignty remains a task for further research.

Overcoming these vulnerabilities is a shared task of at least three actors. Regulators must ensure legally guaranteed and technically implemented access to public data, regardless of which platform or registry is concerned. The corpus indicates where this is hardest: the state is the actor of most restrictions in the sample, and statutory grounds are its usual instrument, so the guarantee has to be built against the same mechanism that most often removes access. Journalists and newsrooms must develop a culture of verification and make their methodology transparent to the audience – while recognizing that in this corpus contestation alone did not distinguish restored from unrestored cases, which places the burden on documentation rather than on protest. Universities and educational institutions must integrate data literacy into the training not only of future journalists but of a broad range of professionals who work with information and communication.

The framework proposed here has now been tested on documented material, and the test returned a correction rather than a confirmation: of the four parameters, formal basis and visibility proved to be largely properties of the actor, so in its tested form the framework rests on two – the actor and the affected link. Several directions remain open. The corpus covers a single jurisdiction, so cross-country comparative coding would show whether the patterns observed here are specific to Ukraine. Expert interviews and audience surveys would address what documentary coding cannot reach – how restrictions are experienced by those who encounter them.

ISSN 2312-5160
online ISSN 2786-4502

Prospects for further research are also seen in the thematic dimension: it appears productive to study in greater depth the individual components of the framework – the role of algorithmic and recommendation systems in shaping information overload, as well as the legal and ethical dimensions of access to public data under martial law. An interdisciplinary view is promising, drawing on the approaches of media psychology and perception studies. Beyond the single indicator established here, the concept of informational sovereignty remains open to fuller operationalization – its transformation into a system of measurable indicators suitable for applied research on the resilience of the information environment. Research access to platform data also deserves study. The corpus shows that a transparency requirement can simultaneously widen access within a jurisdiction and entrench its absence outside it: TikTok opened its Research API to researchers in the United States, the European Economic Area, the United Kingdom, and Switzerland, while researchers in Ukraine remained outside these lists (R021).

## Conclusions

The restrictions examined in this article – active ones, which add content, and passive ones, which withdraw it – converge in form but diverge in consequence. The first operates through the production of false narratives and the suppression of alternative voices; the second through the deprivation of the tools of independent verification. Both reach the same link of the citizen's informational capacity: in the great majority of coded events the capacity to verify is affected. They part company in what follows – how long the restriction lasts, whether a procedure for lifting it exists, and who holds that procedure. What differs is not the technique of restriction but the actor and the route back. The framework proposed for describing both forms did not survive the test intact: of its four parameters, only the actor and the affected link proved to vary independently, while the formal basis and the visibility of a restriction turned out to be largely properties of the actor. Artificial intelligence scales both simultaneously: by automating the production of disinformation and pseudo-data, it transforms information overload from a side effect into a consciously controlled instrument.

For data journalism, this means that it is not enough to be able to analyze data – one must have the right to obtain it, the technical capacity to process it, and an audience capable of perceiving it. All three conditions are systemically vulnerable – both in peacetime and especially under conditions of armed conflict.

Informational sovereignty, as the citizen's ability to verify reality independently of the state, platforms, and media intermediaries, is not a purely technical task. It is a cultural and political task. And its resolution begins with the recognition that freedom of speech, without freedom of data and without the capacity to understand it, is incomplete.

**Conflict of Interest.** Not declared.

**Funding.** No funding was received.

**Data Availability Statement.** The data set on which the article is based – a coding workbook containing a codebook, a list of source cases, coded data, and a log of discrepancies – is openly available in the Zenodo repository (https://doi.org/10.5281/zenodo.23627347).

**Author Contributions.** *Yana Shekeriak-Kushka*: conceptualization of the research; design of the research and development of the coding scheme; investigation and data collection (formation of the corpus, search and verification of sources); data curation (development of the codebook, preparation of the dataset); validation of reproducibility (independent coding of the corpus, calculation of intercoder agreement, maintenance of the disagreement log); data analysis; manuscript preparation – original draft (in particular, the parts of the literature review and subsections addressing indirect means of restricting information and the role of data journalism as a tool of counteraction, with an analysis of new vulnerabilities arising from the nature of data

processing and representation in media; identifying the logic underlying structural data closure as a mechanism restricting access to information; description of the research design, coding scheme, and procedure; calculation of distributions, cross-tabulations, and reliability indicators, and interpretation of the coding results); manuscript preparation – review and editing; project administration. *Vladyslav Bilozerov*: conceptualization of the research; selection of research methods; investigation and data collection (formation of the corpus, search and verification of sources); validation of reproducibility (independent coding of the corpus); data analysis; visualization of results; manuscript preparation – original draft (in particular, the parts of the literature review and subsections addressing the development of censorship methods and the contribution of artificial intelligence to new mechanisms of its transformation and scaling; identifying the logic underlying digital censorship and propaganda as mechanisms restricting access to information; interpretation of the coding results); manuscript preparation – review and editing.

**Ethics Approval.** Ethical approval was not required for this study.

**Informed Consent.** Not covered by the study.

**Consent for Publication.** Not covered by the study.

**Declaration of generative artificial intelligence and technologies using artificial intelligence in the writing process.** The authors declare the use of artificial intelligence tools in the preparation of this article. An AI assistant (Claude, Anthropic) was used to generate a draft translation of the Ukrainian text into English (which the authors subsequently edited), to calculate the intercoder reliability (Cohen's κ) based on two independently coded files, to verify the consistency of numerical data between the manuscript and the dataset, and to translate the coding instrument into English. Details regarding the calculation of intercoder reliability are provided in the "Method" section. The selection of the corpus, verification of each instance against primary sources, checking the versions of legal acts in force at the time of each event, development of the research design, creation of the coding scheme, all coding-related decisions, the literature review, formulation of theoretical propositions, the proposed analytical framework, the hypothesis, and the interpretation of results were all carried out by the authors. Both authors coded the corpus independently of each other. The authors bear full responsibility for the content of the manuscript and its supplementary materials, including the accuracy of all numerical data, quotations, and references to sources.

**Permissions.** Not covered by the study.

## References

Accountable Tech. (2024a). *Meta's political content limit causes steep drop in reach for accounts.* https://accountabletech.org/research/metas-political-content-limit-causes-steep-drop-in-reach-for-accounts/

Accountable Tech. (2024b, April 10). *200+ creators call on Instagram to stop limiting "political content" by default.* https://accountabletech.org/statements/200-creators-call-on-instagram-to-stop-limiting-political-content-by-default/

American Sunlight Project. (2025). *A pro-Russia content network foreshadows the automated future of info ops.* https://americansunlight.org/updates/the-american-sunlight-project-unveils-detailed-report-on-the-critical-threat-of-russian-disinformation-in-ai-models

Benkler, Y., Faris, R., & Roberts, H. (2018). *Network propaganda: Manipulation, disinformation, and radicalization in American politics*. Oxford University Press. https://doi.org/10.1093/oso/9780190923624.001.0001

Bermes, A. (2021). Information overload and fake news sharing: A transactional stress perspective exploring the mitigating role of consumers' resilience during COVID-19. *Journal of Retailing and Consumer Services, 61*, Article 102555. https://doi.org/10.1016/j.jretconser.2021.102555

Camaj, L., Lanosga, G., & Martin, J. (2025). A global perspective on data journalism materiality: Knowledge production across public transparency infrastructure environments. *Digital Journalism, 13(3), 418–437.* https://doi.org/10.1080/21670811.2023.2278040

Casas, A., Dagher, G., & O'Loughlin, B. (2025). Commentary: How do we get platforms to share data with independent researchers? Regulation alone will not cut it. *Child and Adolescent Mental Health, 30*(3), 289–291. https://doi.org/10.1111/camh.70020

Chesney, R., & Citron, D. K. (2018). *Deep fakes: A looming challenge for privacy, democracy, and national security*. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213954

Doctors for America v. Office of Personnel Management, 793 F. Supp. 3d 112 (D.D.C. 2025). https://litigationtracker.law.georgetown.edu/wp-content/uploads/2025/05/DRS-FOR-AMERICA_2025.02.11_ORDER-GRANTING-TRO.pdf

Ettinger, M. B. (1971). A solution to the information pollution problem. *Chemical Technology*, (6), 330–331.

European Commission. (2024). Ukraine 2024 report (SWD(2024) 699 final). https://enlargement.ec.europa.eu/document/download/1924a044-b30f-48a2-99c1-50edeac14da1_en

Freedom House. (2024). *Freedom on the net 2024: Ukraine*. https://freedomhouse.org/country/ukraine/freedom-net/2024

Graphite. (2025). *More articles are now created by AI than humans.* https://graphite.io/five-percent/research/more-articles-are-now-created-by-ai-than-humans

Grübl, T., Enguix, F., & Stiller, B. (2026). A review of internet censorship: Modern measurement and circumvention techniques. *Computer Science Review, 62*, Article 101002. https://doi.org/10.1016/j.cosrev.2026.101002

Hameleers, M., Tulin, M., de Vreese, C., Aalberg, T., Van Aelst, P., Cardenal, A. S., Corbu, N., van Erkel, P., Esser, F., Gehle, L., Halagiera, D., Hopmann, D. N., Koc-Michalska, K., Matthes, J., Meltzer, C., Mihelj, S., Schemer, C., Sheafer, T., Splendore, S., … Zoizner, A. (2024). Mistakenly misinformed or intentionally deceived? Mis- and disinformation perceptions on the Russian War in Ukraine among citizens in 19 countries. *European Journal of Political Research, 63*(4), 1642–1654. https://doi.org/10.1111/1475-6765.12646

Hills, T. T. (2019). The dark side of information proliferation. *Perspectives on Psychological Science*, 14(3), 323–330. https://doi.org/10.1177/1745691618803647

Jasser, J. (2023). *Identification and modeling social media influence pathways: A characterization of a disinformation campaign using the flooding-the-zone strategy via transfer entropy* [Doctoral dissertation, University of Central Florida]. Electronic Theses and Dissertations, 2020–2023. https://stars.library.ucf.edu/etd2020/1583/

Jungblut, M., Kümpel, A. S., Peter, C., & Wulf, T. (2023). The Russian invasion of Ukraine in modern information environments: Content, consumers, and consequences of digital conflict communication. *Frontiers in Political Science, 5*, Article 1227005. https://doi.org/10.3389/fpos.2023.1227005

Martin, J. A., Camaj, L., & Lanosga, G. (2024). Scrape, request, collect, repeat: How data journalists around the world transcend obstacles to public data. *Journalism Practice, 18(10), 2477–2494*. https://doi.org/10.1080/17512786.2022.2142837

Ministry of Digital Transformation of Ukraine. (2022, February 23). *Yedynyi derzhavnyi vebportal vidkrytykh danykh: Nabory danykh* [Unified state web portal of open data: Datasets]. Internet Archive. https://web.archive.org/web/20220223165625/data.gov.ua/dataset

Ministry of Digital Transformation of Ukraine. (2023, March 14). *Yedynyi derzhavnyi vebportal vidkrytykh danykh: Nabory danykh* [Unified state web portal of open data: Datasets]. Internet Archive. https://web.archive.org/web/20230314180418/https://data.gov.ua/dataset

Ministry of Digital Transformation of Ukraine. (2026a, February 11). *Yedynyi derzhavnyi vebportal vidkrytykh danykh: Nabory danykh* [Unified state web portal of open data: Datasets]. Internet Archive. https://web.archive.org/web/20260211130136/data.gov.ua/dataset

Ministry of Digital Transformation of Ukraine. (2026b). *Yedynyi derzhavnyi vebportal vidkrytykh danykh: Nabory danykh* [Unified state web portal of open data: Datasets]. https://data.gov.ua/dataset

Ni, T., Zhu, R., & Krever, R. (2023). Responses to news overload in a non-partisan environment: News avoidance in China. *SAGE Open, 13*(3). https://doi.org/10.1177/21582440231184864

Oleksiyuk, T. (2025). The right to access official information as a resilience-improving tool: Ukrainian lessons during wartime. *Social Sciences & Humanities Open, 11*, Article 101549. https://doi.org/10.1016/j.ssaho.2025.101549

Papageorgiou, G., Loukis, E., Magnussen, R., & Charalabidis, Y. (2023). Open data journalism: A domain mapping review. In *Proceedings of the 16th International Conference on Theory and Practice of Electronic Governance (ICEGOV 2023)*. https://doi.org/10.1145/3614321.3614340

Roozenbeek, J., & van der Linden, S. (2019). Fake news game confers psychological resistance against online misinformation. *Palgrave Communications, 5*, Article 65. https://doi.org/10.1057/s41599-019-0279-9

Sadeghi, M., & Blachez, I. (2025, March 6). *A well-funded Moscow-based global "news" network has infected Western artificial intelligence tools worldwide with Russian propaganda.* NewsGuard Reality Check. https://www.newsguardrealitycheck.com/p/a-well-funded-moscow-based-global

Sanderson, Z., Messing, S., & Tucker, J. A. (2024, January 22). *Misunderstood mechanics: How AI, TikTok, and the liar's dividend might affect the 2024 elections. Brookings Institution.* https://www.brookings.edu/articles/misunderstood-mechanics-how-ai-tiktok-and-the-liars-dividend-might-affect-the-2024-elections/

Shekeriak-Kushka, Y., & Bilozerov, V. (2026). *Coding workbook: Restrictions on access to information in Ukraine, 2022–2026* [Data set]. Zenodo. https://doi.org/10.5281/zenodo.23627347

Szegőfi, Á., Altay, S., & Heintz, C. (2026). *"Flooding" using disinformation* [Preprint]. SSRN. https://doi.org/10.2139/ssrn.6216050

Washenko, A. (2025, January 8). Threads and Instagram will recommend political content after all. *Engadget.* https://www.engadget.com/social-media/threads-and-instagram-will-recommend-political-content-after-all-232343107.html

Zheng, H., & Zhan, H. (2026). Science behind a paywall: Restricted access limits the promise of artificial intelligence. *Learned Publishing, 39*(3), Article e2059. https://doi.org/10.1002/leap.2059

# Appendix A

## Supplementary Distributions

**Table A1.** ***Distribution by Actor, Formal Basis, and Visibility (N = 27)***

| Variable | Value | n | % |
|---|---|---|---|
| Actor | state | 16 | 59.3 |
| | platform | 7 | 25.9 |
| | external actor | 4 | 14.8 |
| Formal basis | law | 13 | 48.1 |
| | platform policy | 7 | 25.9 |
| | no basis stated | 7 | 25.9 |
| Visibility | explicit | 12 | 44.4 |
| | discoverable | 12 | 44.4 |
| | concealed | 3 | 11.1 |

**Table A2.** ***Distributions by Character, Duration, Security Justification, and Contestation***

| Variable | Value | n | % |
|---|---|---|---|
| Character (N = 27) | direct | 20 | 74.1 |
| | not applicable | 4 | 14.8 |
| | mixed | 2 | 7.4 |
| | indirect | 1 | 3.7 |
| Duration (N = 26) | ongoing | 16 | 61.5 |

ISSN 2312-5160
online ISSN 2786-4502

| Variable | Value | n | % |
|---|---|---|---|
| | over 1 year | 6 | 23.1 |
| | 1–12 months | 3 | 11.5 |
| | under 1 month | 1 | 3.8 |
| Security justification (N = 26) | not declared | 15 | 57.7 |
| | declared | 8 | 30.8 |
| | declared post hoc | 3 | 11.5 |
| Contestation (N = 27) | contested | 18 | 66.7 |
| | no data | 8 | 29.6 |
| | not contested | 1 | 3.7 |

**Table A3.** ***Type of Restriction × Reversibility (N = 26)***

| Type of restriction | restored | partially | not restored |
|---|---|---|---|
| registry closure | 1 | 5 | 1 |
| narrowing of data scope | 0 | 2 | 5 |
| access blocking | 1 | 0 | 3 |
| API termination | 0 | 1 | 2 |
| information noise (flooding) | 0 | 0 | 3 |
| algorithmic downranking | 1 | 0 | 0 |
| deferral of publication | 0 | 0 | 1 |

A secondary type of restriction was recorded in 9 events: narrowing of data scope (5), access blocking (2), content removal (1), and deferral of publication (1). Secondary types do not enter the frequency distribution of principal types.

**Table A4**. ***Combinations of Affected Links (N = 27)***

| Combination | n | % |
|---|---|---|
| production + verification | 20 | 74.1 |
| perception only | 3 | 11.1 |
| perception + verification | 2 | 7.4 |
| production + perception + verification | 2 | 7.4 |

**Table A5.** ***Actor × Reversibility (N = 26)***

| Actor | restored | partially restored | not restored | Total |
|---|---|---|---|---|
| state | 0 | 7 | 8 | 15 |
| platform | 2 | 1 | 4 | 7 |
| external actor | 1 | 0 | 3 | 4 |

ISSN 2312-5160
online ISSN 2786-4502

# Appendix B

## List of Coded Cases

**Table B1.** ***Main Corpus: Restriction Events in Ukraine, February 2022 – January 2026***

| ID | Onset | Actor | Basis | Event |
|---|---|---|---|---|
| R001 | 24 Feb 2022 | state | no basis stated | Asset declarations register closed to public access |
| R002 | 24 Feb 2022 | state | no basis stated | Unified State Register of Court Decisions switched off |
| R004 | 13 Apr 2022 | state | law | Ministry of Justice Order No. 1462/5 suspending open data publication |
| R005 | 5 Mar 2022 | state | law | Prozorro: wartime procurement reporting deferred (Resolution No. 201) |
| R006 | 24 Feb 2022 | state | no basis stated | National open data portal data.gov.ua switched off |
| R007 | 18 Nov 2025 | state | law | Law No. 4576-IX restricting access to nine public registers |
| R008 | 19 Jan 2026 | – | – | Company register data restored with fields removed |
| R009 | 4 Dec 2024 | state | law | Draft Law No. 10242 criminalizing use of register data (not enacted) |
| R010 | Feb 2022 | state | law | State Statistics Service suspended publication of statistics |
| R011 | 22 Jun 2022 | state | law | Defense-sector data restricted on the public funds portal |
| R012 | Nov 2025 | state | law | Statistics on military offences restricted |
| R014 | 3 Mar 2022 | – | – | Commander-in-Chief Order No. 73 on interaction with media |
| R015 | 19 Mar 2022 | state | law | “Yedyni Novyny” telethon as the sole broadcasting format |
| R016 | 9 Feb 2023 | platform | platform policy | Twitter/X ends free API access |
| R017 | 30 Jun 2023 | platform | platform policy | X requires authentication and introduces rate limits |
| R018 | 2 May 2023 | platform | platform policy | Public access to the Pushshift archive (Reddit) withdrawn |
| R019 | 14 Aug 2024 | platform | platform policy | Meta closes CrowdTangle |
| R020 | 14 Aug 2024 | platform | platform policy | Meta Content Library replaces CrowdTangle, access by application |
| R021 | 20 Jul 2023 | platform | platform policy | TikTok Research API limited to a list of jurisdictions |
| R023 | May 2022 | external actor | no basis stated | Doppelgänger / RRN network of cloned media outlets |

ISSN 2312-5160
online ISSN 2786-4502

| ID | Onset | Actor | Basis | Event |
|---|---|---|---|---|
| R024 | Feb 2022 | external actor | no basis stated | Portal Kombat / Pravda network |
| R025 | 1 Aug 2023 | external actor | no basis stated | Matryoshka campaign impersonating media and academics |
| R026 | 19 Dec 2024 | external actor | no basis stated | Cyberattack on Ministry of Justice registers |
| R027 | Mar 2024 | platform | platform policy | Meta limits recommendation of political content by default |
| R028 | 4 Apr 2022 | state | law | TV channels disconnected from DVB-T2 under sanctions |
| R029 | 15 Nov 2022 | state | law | Defense procurement withdrawn from public access (Resolution No. 1275) |
| R030 | 19 Oct 2022 | state | law | Mechanism for terminating public access in Prozorro (Resolution No. 1178) |
| R031 | 24 Feb 2022 | state | law | Public cadastral map and land registry data withdrawn |
| R032 | 24 Feb 2022 | state | law | State Voter Register temporarily suspended |

***Note*. R008 and R014 fall outside the object of study and are not coded; R009 is an attempted restriction that was not enacted and is coded on a reduced set of variables. For each case the dataset (Shekeriak-Kushka & Bilozerov, 2026) provides the primary source with a URL, the date of public disclosure, the full coding on all variables, and the coder's note documenting how each value was assigned.**

**Table B2.** ***Comparative Cases (Excluded from Quantitative Distributions)***

| ID | Onset | Jurisdiction | Basis | Event |
|---|---|---|---|---|
| C001 | 21 Apr 2022 | Russia | law | Publication of foreign trade statistics suspended |
| C002 | 31 Jan 2025 | United States | executive order | Federal datasets and web pages removed |
| C003 | 18 Mar 2023 | India | law | Mobile internet shutdown in Punjab |

Received 21.08.2026
Approved 19.10.2026
Published 09.11.2026