Monitoring of international legal regulation trends for the development of legislation in the digital economy in Russia

Transfer of personal data from EU to US, deceptive data practices, use of AI in courts

Monitoring No.7 (July 2024)

Monitoring was prepared by a team of experts of the International Best Practice Analysis Department at the Gaidar Institute for Economic Policy (the Gaidar Institute):
Authors:
Maria Girich, Researcher, *Ivan Ermokhin,* Researcher, *Antonina Levashenko,* Senior Researcher, *Olga Magomedova,* Researcher, *Tatiana Malinina*, Senior Researcher.

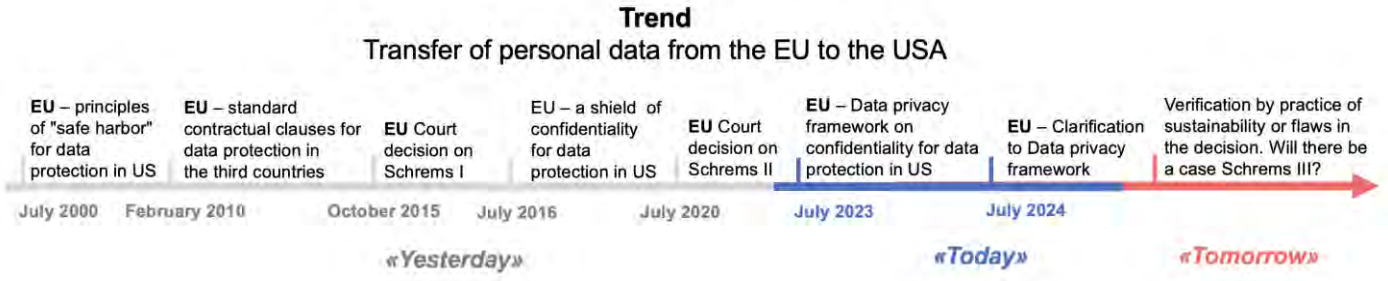
"...words that were completely unimportant were printed in capital letters, and everything that was essential was printed in the smallest font."

Mikhail Saltykov-Schedrin

In July 2024, there are 3 main events that define trends in the development of digital economy regulation.

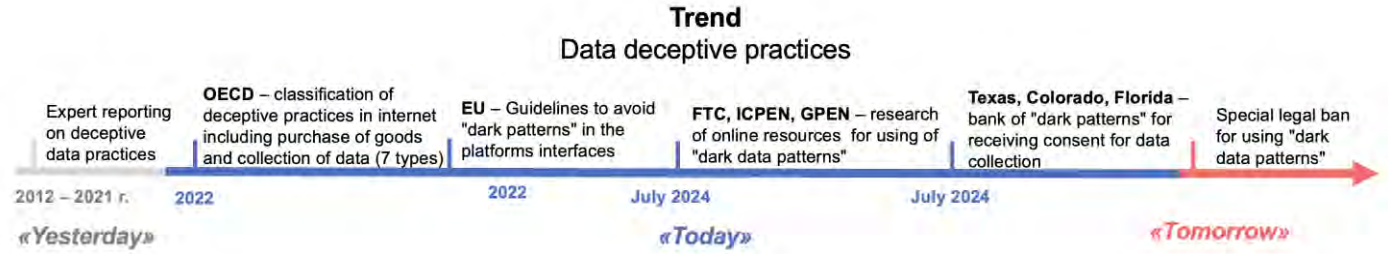
Trend No.1. Transfer of personal data from the EU to the U.S.

In July, the EU published clarifications to the Data Privacy Framework related to confidentiality of data transfer from the EU to the U.S., adopted back in 2023. The mechanisms for implementing this framework are aimed at reducing the risks of excessive access by U.S. intelligence agencies to data transferred from the EU. However, there are doubts as to how this will work.



Trend No.2. Deceptive data practices

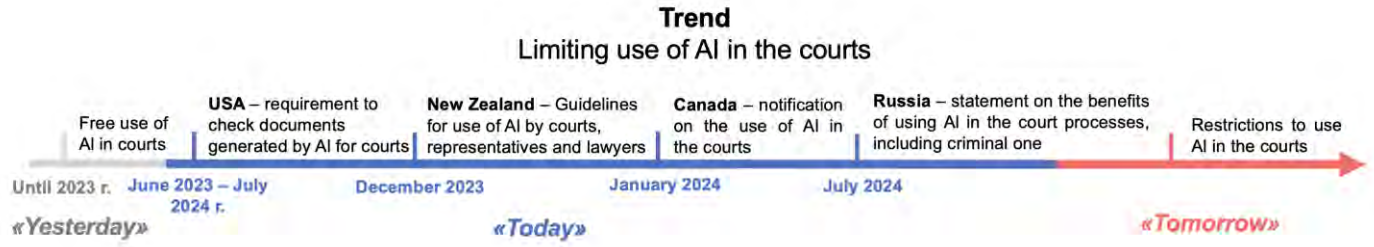
In July, 3 U.S. states banned online platforms from using deceptive ("dark") data practices. According to FTC[1], ICPEN[2], GPEN[3], research, users of more than 1,000 websites have at least once encountered one of the "dark practices" on 97% of resources. Internet resources force users to agree to unprotected data processing methods, fraudulently collect more data than necessary, etc.



[1] US Federal Trade Commission
[2] International Consumer Protection and Enforcement Network
[3] Global Privacy Enforcement Network

Trend No.3. Limiting use of AI in courts

In July, the Supreme Court of the Russian Federation announced that the use of AI in preparing documents in courts would reduce errors in sentencing. However, the U.S. District Court for the Western District of North Carolina expressed caution in the use of AI by courts and parties: every statement and reference to laws, court decisions contained in the document must be verified. As of June 2023, courts in several countries (Canada, New Zealand, Australia) have already issued liability warnings for parties' use of AI in court.



1. Transfer of personal data from the EU to the US

Personal data (hereinafter referred to as PD) are transferred from the EU to companies in the US, including to support international trade (e.g. airline services) and labor market needs (e.g. hiring an EU professional in the US). As a general rule, PD from the EU may be transferred to countries providing adequate PD protection, which may be recognized by European Commission decisions or ensured by certain instruments, such as standard contractual clauses (signed by the companies transferring and receiving PD).[4] As the US PD regulation is less stringent than in the EU, the US was not considered by default to have adequate PD protection. The European Commission's decisions on the adequacy of protection of PD in the US facilitate their cross-border transfer.

Among the documents that formed the basis for the European Commission's decisions on the adequacy of protection is the EU-US Data Privacy Framework. In July 2024, the European Council for Data Protection published clarifications to these provisions[5], specifying technical aspects of PD transfer (e.g., transfer of PD to companies that are subsidiaries of those that have adhered to the framework, obligation to inform data subjects about recipients of data in the US).

The European Commission's decision on the adequacy of US PD protection under the Framework provisions,[6,7] was issued in July 2023, however, 2 decisions of the European Commission similar in form and meaning (the Safe Harbor Principles Decision[8] of 2000 and the Privacy Shield Decision of 2016[9]) were previously in force), which were recognized invalid by the EU Court[10] under cases Schrems I (2015)[11] and Schrems II (2020).[12,13]

The Safe Harbor, Privacy Shield and Data Privacy Frameworks are based on the principles of information, accountability in onward transmission, security of transmission, data integrity, etc.[14] There are slight differences in the “safe harbor” and “privacy shield” principles. The latter is broader, e.g. in terms of liability when transferring PD for processing to contractors[15] and in what cases and what must be notified to PD subjects, including the requirement to disclose PD in response to lawful requests from authorities to ensure national security rights of PD subjects.

Another difference between the three European Commission decisions under consideration is the mechanisms for protecting the rights of PD subjects. Thus, in the case of Schrems I (which overturned the safe harbor decision), the EU Court of Justice ruled that the safe harbor principles (2000) provide insufficient legal protection for PD subjects. Therefore, as part of the next solution, the privacy shield, an ombudsman function was provided, so that EU authorities could submit requests on behalf of subjects of PD transferred from the EU using ombudsman in case US intelligence poses risks of a PD violation (e.g., mass collection of PD).

The European Commission's decisions based on the safe harbor and privacy shield principles were invalidated by the EU Court of Justice for the following reasons:

1) disproportionate access by US intelligence agencies to Europeans' PD (e.g., mass collection of PD under the US Foreign Intelligence Surveillance Act);

2) lack of effective legal protection from interference by US government agencies.

[4] In the absence of such decisions and instruments, PD may be transferred from the EU to third countries as an exception: for example, with the expressed consent of the PD subject after being informed of the risks.

[5] https://www.edpb.europa.eu/system/files/2024-07/edpb_dpf_faq-for-businesses_en.pdf

[6] https://eur-lex.europa.eu/eli/dec_impl/2023/1795/oj

[7] The decision means that adequacy of data protection is ensured by the Data Privacy Framework, i.e. it applies only to US companies that have declared compliance with this framework and are therefore listed by the US Department of Commerce, and not to the US as a whole. The same is true for the safe harbor and privacy shield principles.

[8] https://eur-lex.europa.eu/eli/dec/2000/520/oj

[9] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG

[10] Court of Justice of the European Union (CJEU).

[11] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362

[12] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62018CJ0311

[13] Note that this did not create a legal vacuum, as the European Commission's decision on standard contractual clauses (2010, see below) remained in force.

[14]. There are 7 of them: information, selection, accountability in further transfer; security, data integrity and target limitation; access of subjects; defense of rights, enforcement and liability. Principles are published by the U.S. Department of Commerce and are accompanied by negotiations between the EU and the U.S. on the conditions (which also include mechanisms for implementing the principles) on which the adequacy of data protection can be recognized, i.e. the European Commission's decisions are not unilateral.

[15] For example, Facebook transfers users’ data from the EU to its servers in the US; if Facebook in the US conditionally hires company A for processing of these data, then, company A is a contractor.

However, the introduction of the ombudsman function did not affect the effectiveness of legal protection, as he is not, actually, a court.

A decision of the European Commission on the adequacy of protection provided by standard contractual clauses (include, for example, obligations of the data exporter and importer with respect to each other and data subjects) adopted in 2010[16], in the Schrems II case has not been overturned in the court because these provisions, while not binding on third-country authorities, including the US[17], nevertheless, ensure that transfer of PD to a third country is suspended/prohibited if the recipient does not or cannot comply with their protection.

It is worth noting that the decision of the European Commission on the 2023 Data Privacy Framework was taken after the US signed Executive Order No. 14086 in 2022 to strengthen security safeguards in intelligence activities[18], in order to limit disproportionate US intelligence access to European PD. The difference between this solution and the previous two is the introduction of a two-tiered mechanism in the US[19] for consideration of the complaints submitted by PD subjects, whose data were transferred from the EU to the US, with regard to their collection and use by the intelligence:

- - at Level 1, complaints are handled by an official (as opposed to an ombudsman - in the intelligence community, not within the US State Department);
- - at level 2, complaints are handled by a specially created data protection supervisory court, to which a level 1 decision can be appealed. This is intended to strengthen protection against intelligence interference.

These measures are criticized as formal: proportionality is subject to value judgments, and independence, transparency and the impartiality of the data protection supervisory court is challenged because data subjects do not have direct access to it. In this respect, Mr. Schrems prepares for the next hearing in the EU Court.[20] Moreover, both the EU and the US are interested in having a valid decision on the adequacy of the PD protection in the US: for both parties it reduces costs in foreign trade transactions.

Russia's experience

In Russia, according to item 2 Article 12 of the PD Law, the Roskomnadzor has approved the list of countries providing adequate protection of the PD subjects rights: 89 countries[21], including all 27 EU countries, however, there is no US in this list.[22] This means that PD cannot be transferred to the US until Roskomnadzor decides to allow the transfer. Operators have the right to transfer personal data to the countries on the list before the notification of cross-border data transfer is considered by the authorized body, and to other countries as a result of such consideration.

The approach of the Russian Federation is more rigorous than in the EU, where the transfer of personal data to third countries is allowed without authorization of the supervisory authority even in the lack of a decision on the adequacy of protection in these countries (for example, based on binding corporate rules or the consent of the subject of personal data after being informed of the risks). Whether it provides greater protection for PD depends on the scrutiny by the competent authority of the conditions in notices of cross-border data transfers.

2. Deceptive data practices

The U.S. experience

In July 2024, amendments to data laws became effective in 3 US states: Texas,[23], Florida[24] and Colorado.[25]. These states have

[16] https://eur-lex.europa.eu/eli/dec/2010/87/oj
[17] Unlike the decisions discussed above, this decision focuses on the transfer of PD to all third countries, but the Schrems II case involved transfer of PD specifically to the United States.
[18] https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities
[19] https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752
[20] https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu

[21] 55 countries, parties to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and 34 countries that are not. The latter are included in the list if their legal provisions and measures to ensure the confidentiality and security of personal data are in line with the provisions of this convention.
[22] The US was absent in the editions of Roskomnadzor's Order No. 274 dated 15.03.2013.
[23] https://capitol.texas.gov/tlodocs/88R/billtext/html/HB00004F.htm
[24] https://flsenate.gov/Session/Bill/2023/262/BillText/er/HTML
[25] https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf

adopted the concept of “dark patterns”, the practices that manipulate the user interface to violate a user's autonomy, i.e., the ability to feel free to make decisions or choices about use of data. For example, consent to personal data transactions obtained fraudulently; practices designed to collect information from children beyond what is required to receive a service; or an offer to opt out of data protection in a game or social media site.

It also establishes the authority of the Federal Trade Commission to determine lists of prohibited practices whose use is considered a violation of the personal data law.

Experience of international organizations and the EC

In July 2024, a study published by the US FTC in collaboration with ICPEN,[26] GPEN,[27] outlines the results of a review of over 1000 websites and apps for the use of “dark patterns”.[28] Earlier, similar studies were organized in 2022 by the OECD[29] and the EU.[30] “Dark patterns” are used in the design of a website to manipulate consumer opinion, for example:

1. Forcing them to provide more personal information than is necessary to receive products or services.

2. Forcing to accept less secure data processing practices.

3. Preventing users from obtaining information about the protection of their data.

The following patterns were estimated:

1) Complex and confusing language - technical or excessively long privacy policies that are difficult to understand. 89% of the resources studied contained either excessively long privacy policies (more than 3000 words) or technical and confusing language that was difficult to read.

2) Interface interference - design elements that affect users' perception and understanding of their actions related to the PD. Identified in 43% of the resources studied. Examples of practices:

- False hierarchy, visually highlighting some interface elements and hiding others, directing users to less secure PD protection operations. For example, a method is proposed that provides less data protection is highlighted by color contrast.

– Selection of “default” data processing options that provide less data protection.

– Use of phrases that may cause guilt in the consumer. 29% of sites discouraged users from deleting accounts with a warning, such as the phrase “if you click ‘Delete User Account’, you will lose your VIP privileges.”

The EU also highlighted the practice of manipulating consumers' emotions. For example, asking you to inform on your location, so that you can supposedly be found by other users and not be alone, although the platform actually collects such data for its own purposes.

3) Persistence - repeated requests for users to take certain actions that may reduce data protection, such as requests to enable notifications or provide the ability to track geolocation. This practice was used by 41% of sites.

The EU also highlights the practice of “overloading,” when a user receives a large number of requests, the user gets tired and agrees to all the proposed options in relation of PD and unintentionally agrees to actions he/she did not want to agree before.

For example, constantly asking for a phone number or access to contacts, making it easier for the user to agree to provide information rather than continually refuse.

4) Creating barriers, such as providing the opportunity to register an account but lacking tools to delete the account or necessity to take inconvenient steps (filling out a long form or sending a written request to the organization) to delete an account; forcing users to make multiple clicks to get information about the use

[26] International Consumer Protection and Enforcement Network (international organization)
[27] Global Privacy Enforcement Network (international organization)
[28] https://www.privacyenforcement.net/system/files/2024-07/GPEN%20Sweep%202024%20-%20%27Deceptive%20Design%20Patterns%27_0.pdf
[29] OECD report on “Dark commercial practices” https://one.oecd.org/document/DSTI/CP(2021)12/FINAL/en/pdf
[30] Guiding principles No.3/2022 on “Dark patterns in the interfaces of the social networks platforms” https://www.edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf

of their PD. The practice was used by 39% of resources.

5) Compulsory use: a requirement to provide more data to access a service than is necessary. For example, creating an account through the use of third-party social networks to gain access to a user's data about that social network's usage. Such practices were used by 26% of resources. The OECD highlights the practice of demanding information, for example, about user contacts for further spamming of consumer contacts, including allegedly on behalf of the consumer.

Russia's experience

Russia has not adopted the concept of "dark patterns" or other equivalents for abusive data collection practices. However, misleading users about the privacy terms of their data may be grounds for sanctions. For example, according to the decision of the Moscow City Court, the LinkedIn platform was blocked in Russia in 2016 for violating the requirement of personal data localization. The court found that LinkedIn collected behavioral data through cookies, but did not comply with localization requirements with respect to the collected data and imposed a condition in the user agreement on the platform's right to transfer all collected data to third parties.[31] Russia has regulations to prevent misleading users in terms of consumer protection legislation and as part of personal data legislation.

It would make sense if Roskomnadzor develops a checklist of signs of "dark patterns" on digital platforms and establishes an open case bank identified on Russian-language platforms based on general regulations and taking into account judicial practice. The open case bank may be supplemented with materials provided by users to inform them of the risks and motivate platforms to adjust their user data collection policies prior to proceedings by Roskomnadzor.

3. AI use in the courts

In Monitoring No.5 we have already considered the use of AI in law enforcement activity. Meanwhile, a new trend is taking shape, that is, limiting the use of AI in litigation. Courts began receiving complaints about AI-generated attorney opinions or party arguments containing references to non-existent court cases, rules of law, or unsupported arguments.

For example, in 2023, the New York District Court imposed a $5000 fine on parties and their representatives for filing ChatGPT-generated written representations that included quotations from at least 6 non-existent court decisions.[32] Another example is the decision of the Tax Chamber Tribunal in the UK 2023: in a tax dispute, the defense used at least 4 references to IRS investigations that did not exist.[33]

Therefore, in July 2024, the U.S. District Court for the Western District of North Carolina[34], restricted the use of AI to help attorneys form opinions.[35] It is stated that factual and legal citations in court documents prepared using AI must be verified by the filing parties. Any document submitted to the Court must be accompanied by a stipulation that:

- No AI was used in the preparation of the document, except for AI embedded in standard online sources of legal databases (as Westlaw, Lex1s).
- Every statement and reference to sources in the document should be checked for accuracy.

Similar guidelines have been adopted by other courts in the US, e.g. Manitoba,[36] Yukon,[37] etc., as well as by courts in a number of other countries, e.g. UK (on

[31] https://mos-gorsud.ru/mgs/services/cases/appeal-civil/details/19d661b0-6b14-48eb-b753-9adbf19fe32a

[32] https://storage.courtlistener.com/recap/gov.uscourts.nysd.575368/gov.uscourts.nysd.575368.54.0_2.pdf

[33] Felicity Harber v The Commissioners for HMRC https://caselaw.nationalarchives.gov.uk/ukftt/tc/2023/1007

[34] Jurisdiction extends to the courts of the Western District of North Carolina

[35] https://www.ncwd.uscourts.gov/sites/default/files/Standing%20Order%20In%20Re-%20Use%20of%20Artificial%20Intelligence2.pdf

[36] Court of Queen's Bench of Manitoba, Practice Direction dated June 23, 2023, "Use of AI in court filings" https://www.manitobacourts.mb.ca/site/assets/files/2045/practice_direction_-_use_of_artificial_intelligence_in_court_submissions.pdf

[37] The Yukon Supreme Court, Using AI tools https://www.yukoncourts.ca/sites/default/files/2023-06/GENERAL-29%20Use%20of%20AI.pdf

the use of chatbots),[38] New Zealand,[39] Australia,[40] etc.

It is being established that when using AI tools in litigation parties and representatives must:

- Understand how the tools work. For example, the quality of the generated legal response depends on the data for chatbot training, as well as the quality of the user's request.
- Comply with privacy rules: any personal information entered into the chatbot is stored and can be used in requests from other users.
- If parties are representing themselves in court on their own (without lawyers) - notify the court of the use of AI in documents, so that participants are aware of the risks.
- Verify the accuracy of information if AI was used to generate the documents.

The text generated by AI, shall be verified, so that:

1) A version of AI that was trained on obsolete data that does not incorporate more recent case law or legislative changes, was not used.

2) The generated information was complete and accurate (did not refer to fictitious court cases or rules).

3) The practices used were applicable to the particular jurisdiction and were not taken from other jurisdictions that have different substantive laws and procedural requirements.

Russia's experience

In July 2024, the website of the Supreme Court of the Russian Federation published its statement on the possibilities to use AI in preparation for court action.[41] Moreover, the idea of connecting AI to the State Automated System "Justice" is under consideration.[42,43]

Nevertheless, it is recommended that the Supreme Court develop requirements for the use of AI in Russian courts, including:

1) Notification of the court and participants in the trial if AI was used to prepare documents during the trial.

2) The requirement to verify the accuracy of all references to legislation, jurisprudence and other sources.

[38] https://www.judiciary.uk/wp-content/uploads/2023/12/AI-Judicial-Guidance.pdf

[39] https://www.courtsofnz.govt.nz/going-to-court/practice-directions/practice-guidelines/all-benches/guidelines-for-use-of-generative-artificial-intelligence-in-courts-and-tribunals/

[40] https://www.supremecourt.vic.gov.au/forms-fees-and-services/forms-templates-and-guidelines/guideline-responsible-use-of-ai-in-litigation

[41] https://www.vsrf.ru/press_center/mass_media/33763/

[42] The State Automated System "Justice" is a geographically distributed automated information system designed to form a unified information space of the courts of general jurisdiction and the system of the Judicial Department under the Supreme Court

[43] https://rg.ru/2023/05/25/robot-pomozhet-rassudit.html