https://doi.org/10.38044/2686-9136-2025-6-8

СТАТЬИ

ТЕМНЫЕ ПАТТЕРНЫ В ЭПОХУ POST-COOKIE: КАК РЕГУЛИРОВАНИЕ ИНТЕРФЕЙСОВ МЕНЯЕТ ЦИФРОВУЮ РЕКЛАМУ В ЕС И США

Д. В. Корж

Аппарат Общественной палаты Российской Федерации
125993, Россия, Москва, Миусская пл., 7-1

Аннотация

Переход к так называемой эпохе *post-cookie*, обусловленный отказом крупнейших технологических компаний от сторонних *cookie-файлов*, существенно изменил архитектуру цифровой рекламы. По мере сужения возможностей традиционного онлайн-трекинга возрастающее значение приобрели интерфейсные практики получения согласия и взаимодействия с пользователем. Именно в этих практиках все чаще проявляются так называемые «темные паттерны». Соответственно возникает необходимость оценить, как различные правовые системы реагируют на подобные вызовы. Поскольку именно ведущие юрисдикции задают ориентиры для глобального регулирования поведения в информационно-телекоммуникационных сетях, в том числе в сети Интернет, ключевую роль здесь играют Европейский союз и Соединенные Штаты Америки. Исходя из обозначенной проблематики в работе анализируются сходства и различия между европейским и американским подходами к регулированию темных паттернов. Поставленная цель обусловила выбор источников и методов исследования, которые включают нормативные правовые акты ЕС и США, практику надзорных органов по защите данных, методические документы, научные публикации, а также результаты собственного эмпирического анализа. Последний охватывал анализ интерфейсных практик на ряде популярных сайтов и сервисов. Полученные результаты показали, что европейская модель основывается на превентивном регулировании, ограничивающем возможность использования манипулятивных практик уже на стадии проектирования интерфейсов, тогда как американская модель преимущественно функционирует по принципу последующего вмешательства. В совокупности это позволило сформулировать вывод о том, что эффективное регулирование цифровой рекламы требует не столько ограничения манипулятивных практик, сколько стимулирования формирования такой архитектуры цифровой среды, которая основывается на принципах предсказуемости, прозрачности и минимизации данных, обеспечиваемых применяемым законодательством и алгоритмами, создаваемыми технологическими компаниями.

Ключевые слова

темные паттерны, манипулятивные интерфейсы, проектирование интерфейсов, цифровая реклама, данные пользователей, персональные данные, ФТК, недобросовестная практика

Конфликт интересов Автор сообщает об отсутствии конфликта интересов.

Финансирование Исследование не имеет спонсорской поддержки.

Для цитирования Корж, Д. В. (2025). Темные паттерны в эпоху post-cookie: как регулирование интерфейсов меняет цифровую рекламу в ЕС и США. *Цифровое право, 6*(2), 72–90. https://doi.org/10.38044/2686-9136-2025-6-8

Поступила: 07.04.25, принята в печать: 21.05.25, опубликована: 30.06.2025

ARTICLES

DARK PATTERNS IN THE POST-COOKIE ERA: HOW INTERFACE REGULATION TRANSFORMS DIGITAL ADVERTISING IN THE EU AND THE US

Denis V. Korzh

Executive Office of the Civic Chamber of the Russian Federation
7-1, Miusskaya Sq., Moscow, Russia, 125993

Abstract

The transition toward the so-called post-cookie era, driven by the decision of major technology companies to abandon third-party cookies, is significantly reshaping the architecture of digital advertising. In the context of narrowing possibilities for conventional online tracking, interface practices for obtaining consent and interacting with users have been gaining importance. However, these practices are increasingly being associated with so-called dark patterns. Accordingly, there arises a need to assess how different legal systems respond to such challenges. Since leading jurisdictions set the benchmarks for global regulation of behavior in information and telecommunication networks, including the Internet, the European Union and the United States play a key role in this process. In this light, the present study examines the similarities and differences between European and American approaches to regulating dark patterns. The stated objective has determined the selection of sources and research methods, which include EU and US legal acts, enforcement practices undertaken by data protection authorities, methodological documents, academic publications, and the results of the author's own empirical analysis. The latter encompassed an examination of interface practices across several popular websites and services. The findings indicate that the European model is based on preventive regulation, which restricts the use of manipulative practices already at the design stage of user interfaces. At the same time, the American model functions predominantly on a post-intervention basis. Taken together, this leads to the conclusion that effective regulation of digital advertising requires the development of a digital environment architecture grounded in the principles of predictability, transparency, and data minimization, rather than on restricting manipulative practices. These processes should be ensured by both applicable legislation and specific algorithms designed by technology companies.

Keywords
dark patterns, manipulative interfaces, interface design, digital advertising, user data, personal data, FTC, unfair practice

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study has no sponsorship.
For citation	Korzh, D. V. (2025). Dark patterns in the post-cookie era: How interface regulation transforms digital advertising in the EU and the US. *Digital Law Journal, 6*(2), 72–90. https://doi.org/10.38044/2686-9136-2025-6-8

Submitted: 7 Apr. 2025, accepted: 21 May 2025, published: 30 June 2025

Введение

В последние годы цифровая реклама претерпела существенные трансформации, обусловленные как технологическими изменениями, так и эволюцией регуляторной среды. Одним из наиболее значимых факторов, повлиявших на архитектуру цифровых платформ, стало последовательное вытеснение сторонних *cookies*[1], представляющих собой традиционный инструмент отслеживания пользовательской активности. Так, крупнейшие технологические корпорации, такие как *Google LLC* и *Apple Inc.*, реализуют стратегии отказа от сторонних *cookie*-файлов (*third-party cookies*), обосновывая свои действия необходимостью усиления защиты персональных данных и соблюдения требований конфиденциальности.

Однако наступление так называемой эпохи *post-cookie* — условного этапа развития цифровой среды, связанного с переходом от сторонних *cookie*-файлов к иным технологиям мониторинга пользовательской активности — не ознаменовало отказа от инвазивных практик цифрового влияния. Наоборот, на смену *cookies* пришли более скрытые, часто непрозрачные технологии и поведенческие практики, включая цифровой отпечаток (*device fingerprinting*)[2], вероятностное отслеживание (*probabilistic tracking*) и архитектурные приемы в пользовательских интерфейсах,

[1] Под *cookies* понимаются небольшие текстовые файлы, хранящиеся на устройствах, подключенных к информационно-телекоммуникационной сети Интернет. Файлы *cookie* могут выполнять различные функции, например запоминать действия пользователя на веб-сайте, отслеживать введенную на таком сайте информацию и аутентифицировать пользователей при доступе к соответствующим онлайн-сервисам. См. об этом, в частности, разъяснения ирландской комиссии по вопросам защиты данных: Irish Data Protection Commission. (2020). *Guidance note: Cookies and other tracking technologies.* https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20tracking%20technologies.pdf

[2] Цифровой отпечаток формируется с учетом таких параметров устройств, как идентификаторы аппаратной части, версия операционной системы, версия установленного на устройстве браузера, и других системных и аппаратных параметров устройства. Основная сложность в его формировании состоит в поиске баланса между уникальностью цифрового отпечатка и частотой изменения параметров, которые применяются для его получения. См.: Стандарт Банка России «Безопасность финансовых (банковских) операций. Обеспечение безопасности финансовых сервисов с использованием технологии цифровых отпечатков устройств» СТО БР БФБО-1.7-2023. Приказ Банка России «О введении в действие стандарта Банка России СТО БР БФБО-1.7-2023» от 1 марта 2023 г. № ОД-335.

направленные на сокрытие реального характера обработки данных или затруднение отказа от ее осуществления[3].

Именно в этом контексте существенно возрос интерес к феномену темных паттернов, представляющих собой манипулятивные элементы дизайна интерфейса, используемые для искажения свободы выбора пользователя и навязывания поведенческих сценариев, выгодных поставщику цифровых услуг.

По данным Европейской комиссии и партнерских организаций[4], в 2023 г. анализ 399 онлайн-магазинов показал, что 40% из них используют как минимум один из трех наиболее распространенных темных паттернов (от скрытых подписок до создания ложного чувства срочности). Еще более масштабное исследование 2022 г., охватившее наиболее популярные сайты и приложения на территории ЕС, выявило, что 97% из них прибегают к манипулятивным интерфейсным практикам[5].

В глобальном контексте, согласно отчету Международной сети по защите и обеспечению соблюдения прав потребителей за 2024 г., 76% проанализированных сайтов и приложений содержат темные паттерны[6].

Сегмент *cookie*-баннеров также демонстрирует системную проблему. Так, согласно некоторым оценкам, 72% баннеров содержат хотя бы один темный паттерн (Berens et al., 2024, p. 8). Результаты другого исследования показывают, что в США техники вроде пристыживания при подтверждении (*confirmshaming*)[7] либо двусмысленных формулировок[8] используются в 80,9% уведомлений о согласии на *cookies* (Li, 2022, p. 570).

В совокупности эти цифры свидетельствуют, что в условиях трансформирующейся цифровой среды, где отказ от *cookies* сопровождается внедрением новых практик обработки данных, несмотря на видимый упор на конфиденциальность, темные паттерны продолжают функционировать как системный и глобальный инструмент сбора данных и воздействия со стороны цифровых платформ.

---

[3] Например, *Mozilla* открыто заявляет, что браузер *Firefox* по умолчанию блокирует известные методы снятия цифрового отпечатка. См.: Firefox. (n.d.). *Firefox blocks fingerprinting*. Retrieved April 4, 2025, from https://www.firefox.com/en-US/features/block-fingerprinting/
Одновременно с этим *Google* разрабатывает инициативу *Privacy Sandbox* с целью создания новых веб-стандартов, которые должны заменить сторонние файлы *cookie*. *Google* указывает, что цель проекта — сделать текущие механизмы отслеживания устаревшими и блокировать скрытые методы отслеживания, такие как цифровой отпечаток (https://privacysandbox.com/intl/en_us/).

[4] Arntz, P. (2023, January 31). *40% of online shops tricking users with "dark patterns".* Malwarebytes. https://www.malwarebytes.com/blog/news/2023/01/european-commission-goes-after-dark-patterns-in-web-shops

[5] Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F., Liva, G., Lechardoy, L., & Rodríguez de las Heras Ballell, T. (2022). *Behavioural study on unfair commercial practices in the digital environment: Dark patterns and manipulative personalisation.* European Commission. https://data.europa.eu/doi/10.2838/859030

[6] International Consumer Protection and Enforcement Network. (2024). *ICPEN Dark Patterns in Subscription Services Sweep*. https://www.icpen.org/sites/default/files/2024-07/Public%20Report%20ICPEN%20Dark%20Patterns%20Sweep.pdf

[7] Пристыживание при подтверждении (*confirmshaming*) является манипулятивной практикой, при которой пользователю внушается чувство вины или стыда за отказ от предоставления согласия, например, посредством формулировок, подразумевающих негативную оценку отказа (Li, 2022, p. 566).

[8] Двусмысленные формулировки представляют собой темный паттерн, который использует неясный или вводящий в заблуждение язык, чтобы побудить пользователя к определенному действию. Например, вместо четкого «согласен» и «не согласен» используются фразы вроде «продолжить с оптимальными настройками», где «оптимальность» не определена.

С правовой точки зрения темные паттерны представляют собой многоаспектное явление, находящееся на пересечении различных сфер правового регулирования, в частности защиты персональных данных, регулирования конкуренции, прав потребителей, а также этики цифрового дизайна[9]. Их правовая квалификация осложняется трансграничной природой цифровых платформ, а также значительными различиями в подходах к регулированию в Европейском союзе и Соединенных Штатах Америки.

В связи с этим в условиях отказа от *cookies* темные паттерны приобретают не столько технологическую, сколько выраженную нормативную релевантность, поскольку становятся инструментом замещения прежних практик сбора данных при одновременном обходе применимых требований, связанных с информированным согласием, прозрачностью и добросовестной коммерческой практикой. На таком фоне закономерно встает вопрос: способны ли действующие правовые инструменты ЕС и США обеспечить эффективное противодействие манипулятивным практикам интерфейсного дизайна, или же темные паттерны становятся способом обхода предписаний нормативно-правового характера, направленных на защиту пользователей?

Соответственно, настоящее исследование направлено как на выявление правовых рисков, порождаемых использованием темных паттернов, так и на анализ инструментов правового реагирования, формирующихся в ответ на это явление.

Следует также отметить, что несмотря на растущий научный и профессиональный интерес к темным паттернам преобладающее большинство исследований концентрируется на их поведенческих и технических аспектах, включая дизайн взаимодействия с пользователем (*user experience design*, или *UX-design*), человеко-компьютерное взаимодействие и поведенческую экономику (Berens et al., 2024). При этом представляется, что наибольший вклад в формализацию понятия «темные паттерны», их типологизацию и эмпирическое обнаружение в интерфейсах внесли работы дизайнеров-исследователей Г. Бригналла, Ч. Грэя и их соавторов (Brignull et al., 2015; Gray et al., 2018).

В то же время правовой анализ данного феномена остается фрагментарным и преимущественно представлен в методических документах контрольных (надзорных) органов. Определенную нормативную базу в этой связи формируют решения национальных органов по защите данных стран ЕС и правоприменительная практика Федеральной торговой комиссии США (далее — ФТК).

Настоящая же работа преследует цель обозначить направления сравнительно-правового исследования регулирования темных паттернов в условиях перехода к архитектуре *post-cookie* цифрового пространства, сочетающего нормативно-правовой анализ с оценкой технологических решений и рыночных моделей поведения цифровых платформ. Тем самым гипотеза этой работы заключается в предположении, что именно различия между правовыми системами ЕС и США в части регулирования защиты данных и защиты прав потребителей определяют степень восприимчивости цифровых платформ к использованию темных паттернов и предопределяют эффективность правового реагирования.

В свою очередь, новизна настоящего исследования заключается в интеграции правовой и технологической перспектив, что позволяет рассматривать темные паттерны не только как проблему дизайна, но и как объект правового регулирования в рамках комплексной политики, ориентированной на обеспечение прозрачности обработки данных и соблюдение принципов добросовестного взаимодействия с пользователями.

[9] Под этикой цифрового дизайна понимается система ценностных ориентиров, предполагающих добросовестность, прозрачность и уважение к автономии пользователя при разработке интерфейсов (Gjorgjieski, 2024, pp. 575–578).

Анализ проблематики и подходов к регулированию

Понятие темных паттернов (*dark patterns*) все чаще оказывается в центре научных и правовых дискуссий о цифровом регулировании.

Впервые введенное дизайнером Гарри Бригналлом в 2010 г., оно охватывает совокупность приемов проектирования пользовательских интерфейсов, направленных на манипулирование поведением пользователя в интересах оператора платформы (Brignull et al., 2015, pp. 21–23). Сущностной характеристикой таких паттернов является сознательное конструирование визуальных или структурных решений интерфейса таким образом, чтобы пользователь принимал решения, противоречащие его собственным предпочтениям, ожиданиям или интересам (Nouwens et al., 2020, p. 3).

В условиях действия Общего регламента по защите данных (*General Data Protection Regulation,* далее также — *GDPR*)[10] особую значимость приобретает вопрос действительности согласия на обработку персональных данных, которое может быть получено с помощью подобных манипулятивных практик. Так, в соответствии со ст. 4(11) и 7(4) *GDPR* согласие должно быть добровольным, конкретным, информированным и недвусмысленным[11], что ставит под сомнение возможность соблюдения этих критериев при использовании темных паттернов.

Существующая научная и практическая литература предлагает различные классификации темных паттернов.

Так, в работах некоторых исследователей предложено как эмпирическое, так и концептуальное обоснование рассматриваемых классификаций (Brignull et al., 2015, pp. 21–23; Gray et al., 2018, pp. 5–9; Kollmer et al., 2023, pp. 202–205; Edidin et al., 2024, pp. 6–7). Однако наиболее распространенные типологии исходят из следующих критериев (рисунок 1):

- обман (например, использование двусмысленных формулировок или визуально замаскированных кнопок);
- принуждение (вынужденные действия, не относящиеся к основной услуге);
- сокрытие (затруднение отзыва согласия или выхода из подписки);
- асимметрия интерфейса (визуальное или структурное преимущество одной опции над другими);
- создание ложной срочности или страха упущенной выгоды.

Например, в сервисе «Кинопоиск» пользователю при регистрации для бесплатного пробного периода необходимо ввести данные банковской карты, и по истечении этого срока подписка продлевается автоматически, что нередко приводит к неожиданным списаниям денежных средств (рисунок 2).

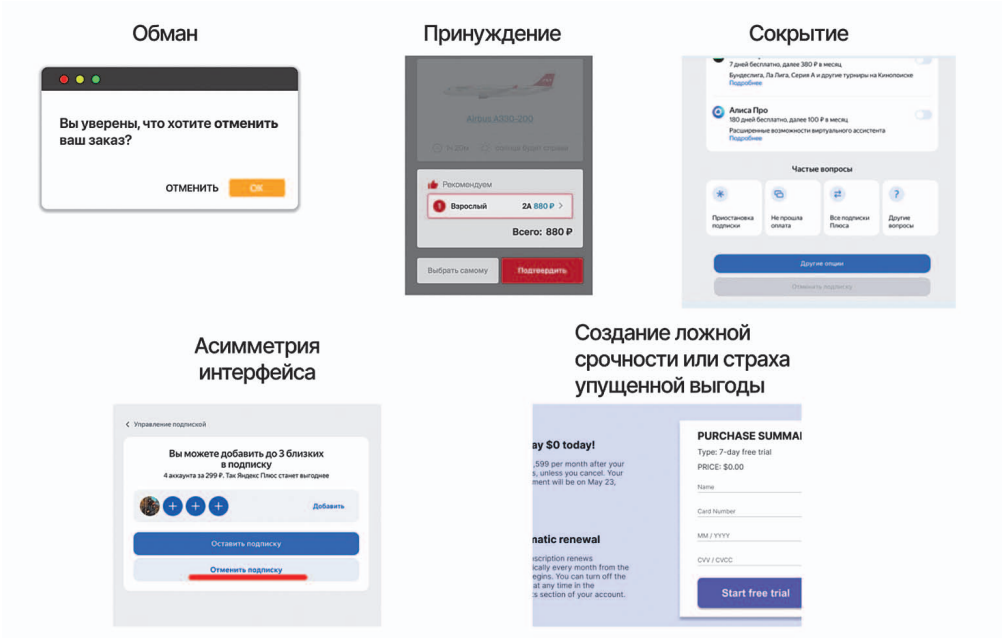
Похожий сценарий можно встретить и при покупке авиабилетов (рисунок 3). Так, например, пользователь выбирает рейс, вводит личные данные, переходит к оплате и внезапно обнаруживает, что стоимость перелета выросла в связи с автоматически активированным страхованием или СМС-информированием либо выбором места на борту самолета. Для отказа от подобных услуг пользователю необходимо вернуться на предыдущий этап и найти малозаметную галочку, спрятанную в интерфейсе.

[10] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1.

[11] General Data Protection Regulation, 2016 O.J. (L 119) 34, 37.

Рисунок 1 / Figure 1

Основные типы темных паттернов / Main types of dark patterns



Примечание. Составлено автором.

Примечательно появление и регуляторных типологий, отраженных, например, в политике ФТК[12] и некоторых разъяснениях европейских надзорных органов по защите данных[13].

Следует отметить, что в условиях постепенного отказа от сторонних *cookie*-файлов, обусловленного как правовыми ограничениями, так и инициативами технологических компаний, интерфейсы становятся основным каналом сбора пользовательских предпочтений и иных данных[14].

Таким образом, архитектура выбора в интерфейсе начинает выполнять регулирующую функцию, способствуя либо соблюдению принципа прозрачности, либо его нарушению. Правовое значение интерфейса как ключевого «пункта входа» в цифровую среду также находит подтверждение в общем направлении правоприменительной практики ст. 6 и 7 *GDPR*[15].

[12] U.S. Federal Trade Commission (2021, April 29). *Bringing dark patterns to light: An FTC workshop.* https://www.ftc.gov/news-events/events/2021/04/bringing-dark-patterns-light-ftc-workshop

[13] См., к примеру, European Data Protection Board. (2023, February 24). *Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them.* https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf

[14] Подобная трансформация связана с тем, что при ограничении традиционных инструментов отслеживания именно интерфейсные решения позволяют собирать согласия, направлять поведение пользователя и косвенно извлекать данные через дизайн-механику взаимодействия.

[15] General Data Protection Regulation, 2016 O.J. (L 119) 36–37.

Рисунок 2 / Figure 2

Пример подключения подписки «Яндекс.Плюс» с обязательным указанием данных банковской карты / An example of activating a "Yandex.Plus" subscription that requires mandatory entry of bank card details

Примечание. Подготовлено автором при обращении к сайту «Яндекс Плюс» (https://plus.yandex.ru/).

При этом проблематика темных паттернов тесно связана с вопросами этики цифрового дизайна, порождая дилемму между дизайном, ориентированным на пользователя, и дизайном, направленным на бизнес-цели, которые зачастую достигаются за счет пользователя.

Впрочем, использование манипулятивных практик ставит под угрозу реализацию основных прав пользователей, включая право на защиту персональных данных. Это особенно проблематично в отношении уязвимых категорий пользователей, в частности несовершеннолетних, пожилых людей, лиц с пониженной цифровой грамотностью, на которых такие приемы могут оказывать непропорционально сильное воздействие. Так, в контексте исследований по когнитивной психологии и поведенческой экономике особое внимание уделяется тому, как архитектура онлайн-выбора взаимодействует с нерефлексивными эвристиками (автоматическими и зачастую неосознаваемыми стратегиями мышления, которыми руководствуется потребитель). Если интерфейс сознательно спроектирован так, чтобы вызвать предвзятость и исказить восприятие выгод и рисков, можно утверждать, что это воздействие направлено

Рисунок 3 / Figure 3

Пример покупки билетов на сайте авиакомпании «Победа», подтверждающий автоматическое предоставление согласия на дополнительные услуги /
An example of purchasing tickets on the "Pobeda" airline website that demonstrates the automatic granting of consent to additional services

Примечание. Подготовлено автором при обращении к сайту авиакомпании «Победа» (https://www.flypobeda.ru).

на подсознательные процессы принятия решений, которые пользователь не способен критически осмыслить.

Поскольку такие процессы не отражают рационального выбора, они не могут служить обоснованием или оправданием принятого решения (Blumenthal-Barby, 2016, pp. 5–15). Именно эта логика лежит в основе аргументации в научной литературе, утверждающей, что автономия личности подрывается присутствием искусственно вызванной предвзятости и манипулятивных эвристик в процессе принятия решений (Brenncke, 2023, pp. 8–9; Cohen, 2019, pp. 33–36, 40–44).

В результате в доктрине усиливается тенденция к переходу от регулирования технических инструментов слежения (таких как *cookie*-файлы) к регулированию самого интерфейса как пространства принятия решения[16]. В этом контексте темные паттерны представляют собой не только технический или дизайнерский феномен, но и правовую категорию, которая требует переосмысления принципов, действующих в рассматриваемой сфере правового регулирования.

С учетом вышеизложенного можно сделать вывод, что одним из наиболее значимых трансформационных процессов в цифровой экономике последних лет является отказ от использования сторонних *cookie*-файлов — технологии, десятилетиями служившей основным инструментом слежения за пользователями и персонализации цифровой рекламы.

[16] См., например: Mathur et al. (2021); Leiser & Santos (2024).

Впрочем, данный сдвиг знаменует собой начало так называемой эпохи *post-cookie*, характеризующейся переосмыслением способов сбора, обработки и монетизации пользовательских данных. Причины же отказа от сторонних *cookie*-файлов носят как нормативный, так и технологический характер. Так, растущая строгость правового регулирования в сфере защиты персональных данных в Европейском союзе и отдельных юрисдикциях Соединенных Штатов Америки сделала невозможным дальнейшее использование *cookie*-файлов в прежнем виде без нарушения положений законодательства в области персональных данных. В частности, Общий регламент по защите данных, принятый в 2016 г., установил в ЕС строгие требования к получению согласия субъектов данных, требуя добровольного, конкретного, информированного и однозначного волеизъявления, посредством которого субъект данных с помощью заявления или четкого утвердительного действия дает согласие на обработку своих персональных данных (ст. 4, 11 *GDPR*)[17], что, как представляется, распространяется и на любые технологии слежения, включая *cookie*-файлы. Аналогичные по содержанию акты стали принимать и в США на уровне штатов. Дополнительные ограничения были закреплены в Директиве о конфиденциальности в электронных коммуникациях (*ePrivacy Directive*)[18].

В свою очередь, технологические корпорации, такие как *Apple Inc.* и *Google LLC*, отреагировали на растущие нормативные и репутационные риски, внедрив собственные ограничения на использование сторонних *cookie*-файлов. Так, *Apple Inc.* реализовала принцип конфиденциальности по замыслу (*privacy by design*)[19] в экосистеме *iOS* в целом и браузере *Safari* в частности, включая обязательное получение согласия через механизм *App Tracking Transparency* (*ATT*)[20]. В то же время *Google LLC* объявила о планомерном отказе от сторонних *cookie*-файлов в браузере *Chrome*, развивая альтернативные инициативы, такие как *Privacy Sandbox* и *Topics API* (https://privacysandbox.com), направленные на менее инвазивные методы персонализации рекламы[21].

Однако следует отметить, что на фоне отказа крупнейших технологических компаний от сторонних *cookie*-файлов бизнес активно адаптируется, развивая альтернативные методы сбора пользовательской информации.

В этой связи одним из ключевых направлений стало усиление роли данных первого уровня (*first-party data*), собираемых бизнесом непосредственно с собственных платформ.

---

17 General Data Protection Regulation, 2016 O.J. (L 119) 33–35.

18 Directive 2002/58/EC, of the European Parliament and of the Council of 12 July 2002 concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications), 2002 O.J. (L 201), 37.

19 Согласно ст. 25 *GDPR* необходимо применять соответствующие технические и организационные меры, такие как псевдонимизация, предназначенные для эффективной реализации принципов защиты данных, таких как минимизация данных, и интеграции необходимых мер безопасности в процесс обработки для соблюдения требований названного Регламента и защиты прав субъектов данных (General Data Protection Regulation, 2016 O.J. (L 119) 48). Иначе говоря, необходимо соблюдать принцип конфиденциальности по замыслу или спроектированной приватности (*privacy by design*).

20 Apple Inc. (n.d.). *User privacy and data use*. Apple Inc. Retrieved April 5, 2025, from https://developer.apple.com/app-store/user-privacy-and-data-use/

21 *App Tracking Transparency (ATT)* является фреймворком, который требует, чтобы приложения получали явное разрешение от пользователя, прежде чем отслеживать его данные на других сайтах и в других приложениях.
В то время как *Privacy Sandbox* представляет собой набор инициатив *Google*, направленный на создание новых веб-стандартов для рекламы. *Topics API* является частью этого набора, которая позволяет браузерам определять интересующие пользователя темы (например, «спорт» или «путешествия») на основе истории его просмотров, не передавая при этом индивидуальные данные.

Представляется, что такие данные менее проблематичны с правовой точки зрения при условии обоснования законных целей их обработки, получения надлежащего согласия и соблюдения иных положений законодательства в области персональных данных.

Параллельно указанной практике развивается контекстная реклама[22], основанная на содержании страницы и параметрах сессии, а не на истории поведения пользователя. Данный подход сравнительно с использованием стандартных *cookie*-файлов представляется менее инвазивным и потенциально более совместимым с положениями законодательства в области персональных данных, однако его коммерческая эффективность все еще обсуждается[23].

Следует обратить внимание на то, что в этих условиях интерфейсные практики приобретают первостепенное значение как способ получения согласия и управления ожиданиями пользователей. В то же время с исчезновением «невидимых» *cookie*-файлов возрастает давление на интерфейс как основной канал коммуникации между пользователем и цифровой платформой.

Это приводит к усилению использования темных паттернов, таких как затруднение или создание препятствий (*obstruction*)[24], асимметрия кнопок согласия[25] и искусственные ограничения в настройках конфиденциальности[26].

Вместе с тем такие интерфейсные решения, формально соответствующие законодательству в области персональных данных, фактически подрывают его эффективность. Именно поэтому темные паттерны становятся значимым правовым и политическим вызовом, создавая иллюзию добровольного согласия при отсутствии реальной свободы выбора.

Учитывая вышеизложенное, важно отметить, что на рассматриваемом этапе развития цифровой среды проблема злоупотреблений в цифровой рекламе не была устранена, а лишь претерпела трансформацию.

---

[22] Контекстная реклама представляет собой тип таргетинга, при котором рекламные объявления показываются в соответствии с содержанием веб-страницы, которую просматривает пользователь. Такой подход не требует отслеживания личных данных и истории поведения.
Дополнительно о механизмах работы контекстной рекламы можно узнать в справочных материалах *Google Ads* (см., например: Google Inc. (n.d.). Контекстный таргетинг. https://support.google.com/google-ads/answer/1726458?hl=ru) или на портале «Яндекс.Директ» (Яндекс Директ. (2024, 1 сентября). *Что такое контекстная реклама и как она работает*. https://direct.yandex.ru/base/articles/kontekstnaya-reklama-chto-eto).

[23] Речь идет о том, что контекстная реклама не обеспечивает того уровня таргетинга и персонализации, который достигается за счет поведенческих данных, поэтому бизнес оценивает ее как менее результативную с точки зрения конверсий и доходности, несмотря на ее большую правовую совместимость с принципами, касающихся обработки персональных данных.

[24] Затруднение или создание препятствий (*obstruction*) представляет собой стратегию создания искусственных препятствий для отказа от *cookies*, включающую усложненные или запутанные процедуры отклонения, направленные на повышение вероятности согласия пользователя.

[25] Асимметрия кнопок согласия является темным паттерном, при котором кнопки согласия и отказа визуально неравнозначны. Например, кнопка «Согласен» может быть выделена ярким цветом и крупным шрифтом, в то время как кнопка «Отклонить» — быть тусклой, мелкой или скрытой в тексте.

[26] Под искусственными ограничениями понимаются приемы, которые создают ложное ощущение дефицита или срочности, чтобы побудить пользователя к немедленному принятию решения, не давая ему времени на обдуманный выбор. Примерами могут служить таймеры обратного отсчета («Предложение действует только 10 минут!») или счетчики остатков товара («Осталось всего 2 штуки!»).

В свою очередь, технологическая замена поведенческого таргетинга усилила значение интерфейсов как ключевого пространства пересечения интересов бизнеса, прав пользователей и деятельности контрольных (надзорных) органов. Анализ же новых форм поведения цифровых платформ и методов их регулирования является необходимым условием для построения этичной и правомерной цифровой среды. Так, обладая комплексной и скоординированной системой регулирования, ЕС развивает модель, включающую как универсальные требования в сфере защиты данных, так и дифференцированные (Santos et al., 2025, pp. 364–367).

Общий регламент по защите данных, хотя и не упоминает напрямую темные паттерны, в то же время создает нормативную основу для их пресечения через принципы минимизации данных и требований к их законной, справедливой и прозрачной обработке (ст. 5(1) *GDPR*)[27].

Важно также учитывать, что в соответствии со ст. 7(3) *GDPR* согласие должно быть легко отзывным и предоставляться без какого-либо принуждения или искажения[28], в результате чего, как представляется, возможность получения действительного согласия с помощью интерфейсных манипуляций исключается.

С принятием Закона о цифровых услугах (*Digital Services Act* (далее — *DSA*))[29] и Закона о цифровых рынках (*Digital Markets Act* (далее — *DMA*))[30], вступивших в силу в 2024 г., регулирование приобрело новое измерение, ориентированное не только на защиту данных, но и на поведенческие аспекты функционирования цифровых платформ. Так, в п. 67 преамбулы *DSA* темные паттерны определяются как онлайн-интерфейсы онлайн-платформ и практики, которые существенно искажают или ухудшают — намеренно или фактически — способность получателей услуг делать самостоятельный и осознанный выбор или принимать решения[31].

В статье же 25 *DSA* закрепляется прямой запрет на использование темных паттернов[32]. В частности, предусматривается, что поставщики онлайн-платформ не должны проектировать, организовывать или эксплуатировать свои онлайн-интерфейсы таким образом, чтобы это вводило в заблуждение или манипулировало пользователями их услуг, или таким образом, чтобы это иным образом существенно искажало или затрудняло возможность пользователей принимать свободные и обоснованные решения.

В свою очередь, *DMA*, в частности в ст. 6, вводит обязательства для «привратников» (*gatekeepers*), включая запрет на навязывание подписок или затруднение отказа от услуг, что может также квалифицироваться как использование темных паттернов[33].

---

27 General Data Protection Regulation, 2016 O.J. (L 119) 35.

28 General Data Protection Regulation, 2016 O.J. (L 119) 37.

29 Regulation 2022/2065, of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), 2022 O.J. (L 277) 1.

30 Regulation 2022/1925, of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), 2022 O.J. (L 265) 1.

31 Digital Services Act, 2022 O.J. (L 277) 18.

32 Digital Services Act, 2022 O.J. (L 277) 58–59.

33 Digital Markets Act, 2022 O.J. (L 265) 34–36.

Вместе эти акты формируют нормативную правовую базу для обеспечения цифровой справедливости (*digital fairness*)[34], где ключевым понятием является «архитектура выбора»[35].

Впрочем, важно обратить внимание на то, что отправной точкой в правовом закреплении проблемы темных паттернов в ЕС стали решения национальных надзорных органов по защите данных в рамках *GDPR*. Так, например, Национальная комиссия по персональным данным и свободам Франции (*Commission nationale de l'informatique et des libertés*) оштрафовала *Google LLC* и *Meta Platforms, Inc.*[36] за *cookie*-баннеры, где принятие было облегчено, а отказ затруднен, что было признано нарушением требований к добровольному, конкретному, информированному и недвусмысленному согласию (ст. 4(11) и 7 *GDPR*)[37] и *ePrivacy Directive*[38]. Решение Комиссии по защите персональных данных Ирландии в отношении *Meta Platforms, Inc.*[39], касающееся персонализированной рекламы, также показало недопустимость введения пользователей в заблуждение относительно оснований обработки данных, что может нарушать не только правила защиты данных, но и принципы конкуренции. Данные решения формируют практику признания незаконными интерфейсных элементов, направленных на обход требований согласия.

В то же время регулирование темных паттернов в США осуществляется в условиях фрагментированной нормативной среды, где компетенции распределены между федеральным уровнем (в первую очередь практика ФТК) и законодательством отдельных штатов[40].

Хотя федеральное законодательство не содержит прямого запрета на использование темных паттернов, ФТК последовательно квалифицирует их как недобросовестные или вводящие в заблуждение действия. Так, в 2022 г. ФТК выпустила разъяснения, прямо указывающие на нарушение темными паттернами норм добросовестной коммерческой практики и стандартов информированного согласия, акцентируя внимание на затруднении отписки, психологическом

[34] В настоящий момент Европейская комиссия активно анализирует действующее законодательство о защите прав потребителей на предмет его пригодности в цифровую эпоху. Данная инициатива, известная как *Fitness Check of EU consumer law on digital fairness*, направлена на оценку того, насколько эффективно текущее законодательство (включая Директиву о недобросовестной коммерческой практике (Directive 2005/29/EC, of the European Parliament and of the Council of 11 May 2005 concerning Unfair Business-to-Consumer Commercial Practices in the Internal Market and Amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive), 2005 O.J. (L 149) 22) противостоит новым вызовам, таким как темные паттерны и манипулятивные интерфейсы. См.: European Commission. (2022, November 28). *Consumer protection: Commission launches a public consultation on the Fitness Check of EU consumer law on digital fairness*. https://ec.europa.eu/newsroom/just/items/767499/en

[35] В работах отдельных авторов (см., например: Kahneman, 2013, pp. 8–29) подробно и последовательно развивается концепция архитектуры выбора (*choice architecture*), которая неизбежно присутствует в любой системе, где пользователям предоставляется выбор.

[36] По решению органов государственной власти Российской Федерации организация *Meta Platforms, Inc.* признана экстремистской, ее деятельность запрещена на территории России.

[37] General Data Protection Regulation, 2016 O.J. (L 119) 34, 37.

[38] Directive on Privacy and Electronic Communications, 2002 O.J. (L 201), 37. См. об этом: Data Privacy Manager. (2022, January 12). *CNIL fines Google and Facebook a total of €210 million over cookies.* https://dataprivacymanager.net/cnil-fines-google-and-facebook-a-total-of-e210-million-over-cookies/

[39] Irish Data Protection Commission. (2023, January 4). *Data Protection Commission announces conclusion of two inquiries into Meta Ireland.* https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland

[40] Federal Trade Commission Act § 5, 15 U.S.C. § 45(a).

давлении, дезориентирующих элементах дизайна и ложном представлении о правах пользователя[41].

В свою очередь, дело в отношении *Amazon.com, Inc.* за использование темных паттернов при оформлении и отмене подписки на *Amazon Prime* стало прецедентным; в нем впервые как часть аргументации явно был использован термин «темные паттерны», определяемые как «обманный интерфейс»[42]. Аналогичный иск был подан против *Adobe Inc.*[43] Особое внимание ФТК уделила и *TikTok Inc.*, выявив элементы интерфейса, затрудняющие изменение настроек конфиденциальности и недобросовестно вовлекающие несовершеннолетних пользователей. Досудебное урегулирование с *TikTok Inc.* включало выплату значительной суммы компенсации и изменения в интерфейсе[44].

На уровне штатов наиболее развитое регулирование по рассматриваемому вопросу представлено в Калифорнии, где впервые в американской практике на уровне закона штата были разрешены вопросы использования темных паттернов (*California Consumer Privacy Act*[45] и *California Privacy Rights Act*[46]). На это же обращают внимание и некоторые исследователи (Tran et al., 2024, pp. 4–5).

Следует отметить, что Агентство по защите конфиденциальности Калифорнии использует термин «темные паттерны» и предлагает критерии их выявления[47]. Аналогичные положения появляются и в законах штатов Колорадо, Коннектикут, Вирджиния и Юта[48], что, как было отмечено выше, свидетельствует о формировании фрагментарного, но в некоторой степени скоординированного подхода к регулированию манипулятивных практик.

Впрочем, важно также подчеркнуть, что данный подход делает практику правоприменения более казуистичной и зависимой от конкретных дел, создавая менее предсказуемую среду для цифровых платформ.

С учетом изложенного следует отметить, что решения французской и ирландской комиссий привели к повсеместному изменению интерфейсов *cookie*-баннеров

---

41 U.S. Federal Trade Commission. (2022, September). *Bringing dark patterns to light*. https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf

42 United States v. Amazon.com, Inc., No. 2:23-cv-00932 (W.D. Wash. filed June 21, 2023).

43 United States v. Adobe Inc., No. 5:24-cv-03630-BLF (N.D. Cal. filed July 11, 2024). См. также: U.S. Federal Trade Commission. (2024, June 17). *FTC takes action against adobe and executives for hiding fees, preventing consumers from easily cancelling software subscriptions* [Press release]. https://www.ftc.gov/news-events/news/press-releases/2024/06/ftc-takes-action-against-adobe-executives-hiding-fees-preventing-consumers-easily-cancelling

44 In Re TikTok, Inc., Consumer Privacy Litig., No. 1:20-cv-04699, ECF No. 161 (N.D. Ill. July 28, 2021).

45 Cal. Civ. Code § 1798.140(l) (2025), https://cppa.ca.gov/regulations/pdf/ccpa_statute.pdf

46 Cal. Code Regs. tit. 11, § 7004(b), (c) (2023), https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf

47 California Privacy Protection Agency. (2024, September 4). *Enforcement Advisory No. 2024-02: "Avoiding Dark Patterns: Clear and Understandable Language, Symmetry in Choice"*. California Privacy Protection Agency. https://cppa.ca.gov/pdf/enfadvisory202402.pdf

В этом документе агентство разъясняет, как применять принципы *California Privacy Rights Act* для выявления и предотвращения темных паттернов, а также подчеркивает, что они оцениваются по их эффекту, а не по намерениям.

48 См.: Colo. Privacy Act, ch. 483, 2021 Colo. Sess. Laws 3180 (codified at Colo. Rev. Stat. § 6-1-1301 et seq. (2023))., Connecticut Data Privacy Act, Pub. Act No. 22-15, 2022 Conn. Acts 109 (Reg. Sess.) (codified at Conn. Gen. Stat. §§ 42-515–525 (2023))., Virginia CDPA (2023), Utah Consumer Privacy Act, 2022 Utah Laws 1911 (codified at Utah Code Ann. §§ 13-61-101–404 (2023).

в Европе[49]. В то же время дела ФТК способствовали реформе интерфейсов на американских сайтах, особенно в сфере электронной коммерции и подписных сервисов[50].

В свою очередь, данные изменения демонстрируют растущее влияние правоприменительной практики на дизайн, ранее считавшийся исключительно сферой ответственности бизнеса и *UX*-команд (*user experience teams*)[51]. Одновременно с этим прослеживается формирование международного тренда на развитие более прозрачных и этичных интерфейсов, где ограничение применения темных паттернов становится важным элементом в обеспечении справедливой и сбалансированной архитектуры платформенного взаимодействия.

Вместе с тем применяемые санкционные режимы в рассматриваемой сфере общественных отношений в анализируемых юрисдикциях все же различаются. Так, при европейском подходе нарушения могут повлечь административные штрафы, в частности, достигающие 4% от глобального годового оборота компании (ст. 83(5) *GDPR*)[52], или до 6% согласно ст. 74 *DSA*[53] и 10% в соответствии со ст. 30 *DMA*[54], что среди прочего создает высокий уровень регуляторного давления.

В свою очередь, при американском подходе санкции, как правило, носят индивидуальный характер и определяются в каждом конкретном деле, однако потенциальные суммы компенсаций и предписания о реструктуризации интерфейсов делают их достаточно эффективным инструментом[55]. При этом различие в правовой природе норм — административного права в ЕС и конкурентного/потребительского права в США — приводит к различной интерпретации границ

---

[49] Например, в декабре 2024 г. французская комиссия по персональным данным и свободам направила формальные уведомления ряду издателей с требованием привести *cookie*-баннеры в соответствие с законодательными требованиями (они должны позволять так же легко отклонять *cookies*, как и принимать их, не иметь вводящего в заблуждение оформления). Данное обстоятельство однозначно побудило веб-ресурсы внести изменения в интерфейсы. См.: CNIL. (2024, December 12). *Dark patterns in cookie banners: CNIL issues formal notice to website publishers.* https://www.cnil.fr/en/dark-patterns-cookie-banners-cnil-issues-formal-notice-website-publishers

[50] Например, в октябре 2021 г. ФТК выпустила заявление об ужесточении регулирования в отношении темных паттернов при оформлении подписок, требуя, чтобы пользовательские интерфейсы предоставляли понятную информацию, обеспечивали добровольное согласие и простой способ отмены. См.: U.S. Federal Trade Commission. (2021, October 28). *FTC to ramp up enforcement against illegal dark patterns that trick or trap consumers into subscriptions* [Press release]. https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap-consumers-subscriptions

В сентябре 2022 г. ФТК опубликовала отчет, в котором демонстрируется рост количества совершенно скрытых или замаскированных интерфейсных приемов. См.: U.S. Federal Trade Commission. (2022, September 15). *FTC report shows rise in sophisticated dark patterns designed to trick and trap consumers* [Press release]. https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers

В июле 2024 г. совместный обзор ФТК, Международной сети по защите и обеспечению соблюдения прав потребителей и Глобальная сеть обеспечения защиты конфиденциальности (*Global Privacy Enforcement Network*) выявил распространенность лишь отдельных темных паттернов. См.: U.S. Federal Trade Commission. (2024, July 10). *FTC, ICPEN, GPEN Announce Results of Review of Use of Dark Patterns Affecting Subscription Services, Privacy* [Press release]. https://www.ftc.gov/news-events/news/press-releases/2024/07/ftc-icpen-gpen-announce-results-review-use-dark-patterns-affecting-subscription-services-privacy

[51] *UX*-команды (*user experience teams*) представляют собой группы специалистов, ответственных за проектирование пользовательского опыта. Их задачей является сделать продукт (сайт, приложение и т. д.) удобным, понятным и эффективным для конечного пользователя.

[52] General Data Protection Regulation, 2016 O.J. (L 119) 83.

[53] Ст. 74 *DSA* (Digital Services Act, 2022 O.J. (L 277) 94).

[54] Ст. 30 *DMA* (Digital Markets Act, 2022 O.J. (L 265) 51–53).

[55] Как, например, в вышеупомянутых делах Adobe, No. 5:24-cv-03630-BLF (N.D. Cal.), Amazon, No. 2:23-cv-00932 (W.D. Wash.).

допустимого. Так, в отличие от европейского подхода, где активно формируется превентивная (*ex ante*) модель с детальной регламентацией интерфейсных решений (например, как было отмечено выше, положения *GDPR, DSA* и *DMA* формулируют детализированные запреты и обязанности, которые ограничивают использование манипулятивных интерфейсных решений), американский подход преимущественно строится на регулировании *ex post* (как указывалось выше, в практике ФТК и законодательстве отдельных штатов), представляющем собой такой способ правоприменения, при котором соответствующие категории носят оценочный характер и позволяют квалифицировать поведение как недопустимое только после выявления последствий для конкуренции или потребителей[56].

Таким образом, сравнительный анализ подходов ЕС и США выявляет как сходство (консенсус относительно недопустимости манипулятивного поведения), так и различие (универсализм в ЕС и фрагментарность в США, превентивные меры в ЕС и регулирование *ex post* в США) между ними.

Вместе с тем на фоне изложенного особенно важно подчеркнуть, что проблема темных паттернов требует не столько применения мер регулирования *ex post*, реализуемых посредством правоприменительной практики, сколько формирования превентивных мер, направленных на предотвращение манипуляций на этапе разработки интерфейсных решений.

Так, опираясь на результаты анализа, можно предложить несколько взаимодополняющих подходов, направленных на ограничение манипулятивных практик и укрепление пользовательской автономии. В частности, в условиях продолжающегося отказа от сторонних *cookie*-файлов, повышения интенсивности регулирования и общественного запроса на этичную цифровую среду целесообразным представляется развитие как технологических, так и правовых инструментов обеспечения баланса между интересами бизнеса, государства и пользователей. Одним из таких перспективных направлений видится внедрение принципов этичного дизайна в процессы разработки пользовательских интерфейсов, ставящего во главу угла автономию пользователя, прозрачность обработки данных и минимизацию рисков.

Указанное включает создание симметричных интерфейсов выбора, отказ от предустановленных опций, визуальное равновесие кнопок согласия, а также структурирование контента без создания ложного ощущения срочности или давления. В литературе подобные решения описываются как примеры так называемых «светлых паттернов» (см., к примеру, Edidin et al., 2024, p. 26).

Как уже было отмечено, принцип конфиденциальности по замыслу (*privacy by design*) является нормативно закрепленным ориентиром для минимизации воздействия на поведенческую автономию пользователя[57]. Технологическим же дополнением к реализации этого принципа представляется использование искусственного интеллекта и автоматизированных инструментов пользовательского аудита интерфейсов (*user experience audit*, или *UX audit*)[58] для выявления темных паттернов, которые могут быть интегрированы в процедуры

[56] В юридической литературе термин *«ex ante»* применяется для обозначения превентивных механизмов регулирования, действующих до возникновения нарушения и направленных на предупреждение потенциальных злоупотреблений (например, установление стандартов проектирования интерфейсов). Напротив, *«ex post»* означает меры, принимаемые после совершения нарушения, такие как расследования, судебные иски и санкции (Baldwin et al., 2011).

[57] Этому посвящена ст. 25 *GDPR*. См.: General Data Protection Regulation, 2016 O.J. (L 119) 48.

[58] Пользовательский аудит интерфейсов представляет собой систематическую оценку интерфейсных решений на предмет их соответствия нормативным требованиям, стандартам юзабилити и этическим принципам проектирования.

оценки воздействия (*data protection impact assessment*) и использоваться для внутреннего контроля[59].

В свою очередь, одним из направлений институционального развития может стать сертификация пользовательских интерфейсов и поведенческих моделей цифровых платформ, включая создание отраслевых стандартов, разработку чек-листов и участие сторонних лиц в оценке интерфейсных решений. Такой подход может позволить системно сдерживать манипулятивное поведение до его выхода на рынок[60].

В то же время бизнесу необходимо выстраивать более сбалансированные модели монетизации, совместимые с правами пользователей (например, контекстную рекламу и работу с данными первого уровня (*first-party data*)), исходя из добросовестных и обоснованных пользовательских отношений. В этом контексте темные паттерны утрачивают свою эффективность, поскольку экономика внимания смещается к формированию доверительных связей с пользователем[61].

Таким образом, перспективы регулирования рекламы на современном этапе развития сферы информационно-коммуникационных технологий определяются не столько запретом отдельных практик, сколько формированием согласованной архитектуры цифровой среды, основанной на уважении автономии пользователя. Как представляется, в центре этой архитектуры должны находиться ключевые принципы предсказуемости, прозрачности и минимизации данных, обеспечиваемые применяемым законодательством и алгоритмами, создаваемыми технологическими компаниями.

В то же время синергия этичного дизайна, возможностей искусственного интеллекта и правовых гарантий защиты прав пользователей может создать условия, при которых цифровая реклама перестанет зависеть от манипуляций и перейдет к взаимным ответственности и доверию.

Заключение

Учитывая вышеизложенное, важно подчеркнуть, что феномен темных паттернов представляет собой значимую правовую проблему, возникшую на фоне трансформации цифровой рекламы и перехода к так называемой эпохе *post-cookie*. Изначально являясь проблемой дизайна пользовательских интерфейсов, темные паттерны приобрели выраженную нормативную релевантность в связи с их широким применением для обхода требований к получению согласия, сокрытия реальных практик обработки данных и создания неравных условий при осуществлении выбора пользователем.

Проведенное сравнительно-правовое исследование позволило прийти к ряду ключевых выводов, касающихся правовых рисков, существующих подходов к регулированию в Европейском

[59] Включение автоматизированных инструментов пользовательского аудита интерфейсов в процедуры оценки воздействия позволяет не только повысить эффективность выявления манипулятивных практик, но и продемонстрировать соблюдение организациями принципа подотчетности, закрепленного, в частности, в ст. 7 *GDPR* (См.: General Data Protection Regulation, 2016 O.J. (L 119) 37).

[60] Имеется в виду использование превентивных механизмов контроля качества, сопоставимых с практикой сертификации в иных высокорисковых сферах (например, в области медицинских изделий или финансовых услуг), что позволяет минимизировать риски для пользователей еще до начала массового применения соответствующих решений.

[61] Подобный сдвиг отражает тенденцию к переориентации бизнес-моделей с краткосрочной максимизации кликов и конверсий на долгосрочное укрепление пользовательской лояльности, что соответствует как принципам, касающимся обработки персональных данных, так и экономической логике устойчивого цифрового рынка.

союзе и Соединенных Штатах Америки, а также перспектив борьбы с манипулятивными интерфейсными практиками, среди которых видится необходимым отметить следующие.

1. Отказ от сторонних *cookie*-файлов и смещение фокуса на интерфейс как основной инструмент взаимодействия с пользователем привели к значительному возрастанию значимости темных паттернов. Они стали ключевым способом обхода требований к информированному согласию и прозрачности обработки данных, что обусловило активизацию деятельности контрольных (надзорных) органов в обеих анализируемых юрисдикциях.
2. Темные паттерны представляют собой многоаспектное правовое явление, затрагивающее сферы защиты данных, конкурентного права, прав потребителей и этики цифрового дизайна.
   В ЕС они рассматриваются преимущественно как нарушения положений действующего законодательства, касающихся действительности согласия и прозрачности обработки данных. В США ФТК квалифицирует их как недобросовестные или вводящие в заблуждение коммерческие практики.
3. Анализ судебных и административных споров в ЕС и США показал, что правоприменительная практика оказывает значительное влияние на поведение цифровых платформ и способствует реформированию интерфейсных решений в сторону большей прозрачности и уважения к выбору пользователя.
4. Применение исключительно мер регулирования *ex post*, реализуемых посредством правоприменительной практики, недостаточно — необходимо создание превентивных мер, направленных на предотвращение манипуляций на этапе разработки интерфейсных решений.
5. Несмотря на различия в правовых системах и подходах, наблюдается формирование общего международного вектора в сторону признания недопустимости манипулятивного интерфейсного поведения и необходимости обеспечения прозрачности обработки данных и защиты автономии пользователя.

В заключение представляется важным подчеркнуть, что на современном этапе развития сферы информационно-коммуникационных технологий в условиях, когда интерфейс выступает ключевым элементом взаимодействия с пользователем, комплексное решение проблемы темных паттернов является необходимым условием для построения сбалансированной, этичной и правомерной цифровой среды.

Список литературы / References

1. Baldwin, R., Cave, M., & Lodge, M. (2011). *Understanding regulation: Theory, strategy, and practice* (2nd ed.). Oxford University Press. https://doi.org/10.1093/acprof:osobl/9780199576081.001.0001
2. Berens, B. M., Bohlender, M., Dietmann, H., Krisam, C., Kulyk, O., & Volkamer, M. (2024). Cookie disclaimers: Dark patterns and lack of transparency. *Computers & Security, 136*, Article 103507. https://doi.org/10.1016/j.cose.2023.103507
3. Blumenthal-Barby, J. S. (2016). Biases and heuristics in decision making and their impact on autonomy. *The American Journal of Bioethics, 16*(5), 5–15. https://doi.org/10.1080/15265161.2016.1159750
4. Brenncke, M. (2024). Regulating dark patterns. *Notre Dame Journal of International & Comparative Law*, *14*(1), 39–79.
5. Brignull, H., Miquel, M., Rosenberg, J., & Offer, J. (2015). Dark patterns-user interfaces designed to trick people. *In Proceedings of the Poster Presentation, Australian Psychological Society Congress*, 21–23.

6. Cohen, J. (2019). Bringing down the average: the case for a "less sophisticated" reasonableness standard in US and EU consumer law. *Loyola Consumer Law Review*, 32(1), Article 2.
7. Edidin, B., Kochetkova, K., & Sarankina, N. (2024). Digital abuse: How dark patterns manipulate our lives. *Legal Issues in the Digital Age*, *5*(4), 4–27. https://doi.org/10.17323/2713-2749.2024.4.4.27
8. Gjorgjieski, V. (2024). Ethical standards in graphic design. *Knowledge International Journal*, *66*(5), 575–578.
9. Gray, C., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. (2018). The dark (patterns) side of UX design. In R. Mandryk (Ed.), CHI EA '18: Extended abstracts of the 2018 CHI Conference on Human Factors in Computing Systems (Article 534). *Association for Computing Machinery*. http://dx.doi.org/10.1145/3173574.3174108
10. Kahneman, D. (2013). Foreword. In E. Shafir (Ed.), The behavioral foundations of public policy (pp. VII–IX). *Princeton University Press*.
11. Kollmer, T., & Eckhardt, A. (2023). Dark patterns. *Business & Information Systems Engineering*, 65(2), 201–208. https://doi.org/10.1007/s12599-022-00783-7
12. Leiser, M., & Santos, C. (2024). Dark patterns, enforcement, and the emerging digital design acquis: Manipulation beneath the interface. *European Journal of Law and Technology*, 15(1), 1–30. https://ejlt.org/index.php/ejlt/article/view/990
13. Li, D. (2022). The FTC and the CPRA's regulation of dark patterns in cookie consent notices. *The University of Chicago Business Law Review*, 1(1), 561–590.
14. Mathur, A., Mayer, J., & Kshirsagar, M. (2021). What makes a dark pattern... dark?: Design attributes, normative considerations, and measurement methods. In Y. Kitamura, A. Quigley, K. Isbister, T. Igarashi (Eds.), *CHI EA '21: Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems* (Article 360). Association for Computing Machinery. https://doi.org/10.1145/3411764.3445610
15. Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark Patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In R. Bernhaupt, F. Mueller, D. Verweij, J. Andres (Eds.), *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)* (pp. 1–13). Association for Computing Machinery. https://doi.org/10.1145/3313831.3376321
16. Santos, C., Morozovaite, V., & De Conca, S. (2025). No harm no foul: How harms caused by dark patterns are conceptualised and tackled under EU data protection, consumer and competition laws. *Information & Communications Technology Law,* 34(3), 329–375. https://doi.org/10.1080/13600834.2025.2461958
17. Tran, V. H., Mehrotra, A., Sharma, R., Chetty, M., Feamster, N., Frankenreiter, J., & Strahilevitz, L. (2024). *Dark patterns in the opt-out process and compliance with the California Consumer Privacy Act (CCPA).* ArXiv. https://doi.org/10.48550/arXiv.2409.09222

Сведения об авторе:

Корж Д. В. — магистр права, факультет права, Национальный исследовательский университет «Высшая школа экономики»; юрист-аналитик, Аппарат Общественной палаты Российской Федерации, Москва, Россия.
dvkorzh@icloud.com
ORCID: https://orcid.org/0009-0002-0624-7664

Information about the author:

Denis V. Korzh — LL.M, Faculty of Law, HSE University; lawyer-analyst, Executive Office of the Civic Chamber of the Russian Federation, Moscow, Russia.
dvkorzh@icloud.com
ORCID: https://orcid.org/0009-0002-0624-7664