ФИЛОСОФСКИЕ АСПЕКТЫ СОГЛАСИЯ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Колесинский А.Д., магистрант

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Чуешов В.И. – д-р фил. наук, профессор

Рассматриваются философские аспекты персональных данных и института согласия на их обработку в условиях цифрового общества. Анализируется взаимосвязь между правом на приватность, автономией личности и механизмом согласия как юридическим инструментом контроля человека над информацией о себе. Особое внимание уделяется философско-правовым основаниям института согласия, его отражению в международных правовых актах и национальном законодательстве, а также проблемам его реализации в современной цифровой среде. Рассматриваются современные вызовы, связанные с развитием технологий обработки данных, включая информационную асимметрию, формальность согласия и коммерциализацию персональной информации. Делается вывод о необходимости совершенствования института согласия и разработки дополнительных механизмов защиты прав человека в сфере обработки персональных данных.

Философское обоснование согласия на обработку персональных данных уходит корнями в фундаментальные представления о личной автономии и человеческом достоинстве. Уже в классической работе Уоррена и Брандайса приватность определялась как право быть оставленным в покое, что подчеркивало суверенное господство индивида над информацией о себе [1]. Американский политолог Алан Уэстин развил эту идею, трактуя приватность как право личности самой решать, какие сведения о ней раскрываются другим и на каких условиях [2]. В континентальной Европе этот подход получил юридическое выражение в доктрине информационного самоопределения, сформулированной Федеральным конституционным судом Германии в 1983 году. Суд указал, что в условиях современных технологий защита личности от неограниченного сбора и использования ее данных вытекает из основного права на свободное развитие личности и человеческое достоинство, гарантируя возможность индивида контролировать раскрытие своих персональных данных [3]. Данный прецедент заложил философско-правовой фундамент всей последующей системы законодательства о персональных данных в Европе. Белорусская правовая система также гарантирует неприкосновенность частной жизни, Конституция РБ в статье 28 утверждает право каждого гражданина на частную жизнь и тайну [4]. Как следствие, согласие субъекта выступает краеугольным камнем законного обращения с личными данными, вытекающим из общего права на приватность. Оно отражает принцип автономии личности, способность каждого самостоятельно распоряжаться сведениями о себе.

Однако в цифровую эпоху механизм согласия сталкивается с серьёзными вызовами на практике. Многие исследователи и эксперты указывают на кризис информированного согласия в цифровую эпоху. Согласно букве закона, согласие должно быть информированным, то есть субъекту должны быть разъяснены цели, объём и последствия обработки [5]. Но на практике объём информации, предлагаемый субъекту, настолько велик и сложен, что фактически средний человек не в состоянии его адекватно воспринять. Исследование Л. Кранор и А. Макдональд наглядно показало, чтобы прочитать все политики конфиденциальности, с которыми пользователь сталкивается в сети за год, потребовалось бы около 244 часов, то есть 30 рабочих дней, если читать по 8 часов в день [6]. Очевидно, что ни один человек не может уделить столько времени чтению юридических текстов онлайн. В результате большинство пользователей либо вообще не читают условия, либо просматривают их бегло. Это приводит к явлению, которое можно назвать фиктивной информированностью, человек ставит галочку или нажимает «Согласен», полагая, что так надо, но не усваивает реально, на что именно он дал согласие [7]. Как метко отмечают исследователи, в таких условиях так называемое информированное согласие вырождается в юридическую фикцию [7]. Пользователь совершает действие согласия, не будучи действительно информирован, следовательно, отсутствует та осознанность, которая требовалась юридически.

Другая серьезная проблема связана с отсутствием реальной свободы выбора, когда согласие де факто становится не добровольным. Формально пользователь волен не соглашаться, но практически отказ означает невозможность воспользоваться нужным сервисом или сайтом. Многие мобильные приложения при установке требуют согласиться с обработкой данных, иначе попросту не работают. Такая ситуация получила название принуждение к согласию. GDPR пытался решить эту проблему нормой о недопустимости ставить предоставление услуги в зависимость от согласия на избыточные данные, но на практике грань между необходимыми и избыточными данными не всегда очевидна [8]. Компании нередко включают в пользовательские соглашения условия об обширной обработке данных, обосновывая это неотъемлемостью для функционирования сервиса. Пользователь оказывается перед дилеммой либо принять пакет условий целиком, либо отказаться от сервиса. Естественно, в большинстве случаев он предпочитает согласиться, и вот уже номинально добровольное согласие получено, хотя по сути оно дано под давлением обстоятельств. Проблема усугубляется тем, что в

современном мире некоторые цифровые сервисы стали монополистически необходимыми, отказаться от них крайне сложно, а значит пользователь вынужден акцептовать любые их условия. В литературе по этому поводу говорят об асимметрии сил между корпорациями и индивидами, пользователь технически свободен сказать нет, но социально и практически эта свобода иллюзорна. По выражению Ш. Зубофф, в эпоху капитализма слежки наше согласие превращается в фикцию, технологические гиганты тихо собирают массивы личных сведений, заявляя, что мы сами на это согласились, хотя в действительности мы не контролируем этот процесс [9]. Зубофф называет такое состояние атакой на автономию человека, когда сбор данных стал повсеместным и неотвратимым, говорить о сознательном согласии уже нельзя [9].

Ещё одним феноменом является усталость от необходимости принимать решения о приватности. Столкнувшись с бесконечным потоком всплывающих окон, запросов согласия на cookies, длинных пользовательских соглашений, люди начинают испытывать раздражение и апатию. Вместо обдумывания они механически нажимают «Согласен», лишь бы поскорее получить доступ к нужному контенту. Эмпирические исследования подтверждают, многие пользователи осознают риски для приватности, но чувствуют бессилие контролировать ситуацию и потому намеренно игнорируют детали, соглашаясь по умолчанию [8]. Такая усталость подтачивает саму идею согласия как осознанного акта. По сути, мы имеем массовое явление формального согласия, когда субъекты утрачивают мотивацию защищать свои данные, чувствуя, что это бесполезно или слишком утомительно. Причины такого явления кроются в когнитивной перегрузке, человек просто не способен обрабатывать столько запросов. Согласно теориям поведенческой экономики, избыточный выбор и частые прерывания внимания ведут к ухудшению качества принимаемых решений. Даниэль Солов назвал эту ситуацию дилеммой согласия, с одной стороны, согласие часто не является значимым, но с другой, если отказаться от него, это еще хуже, потому что тогда вообще убирается последний элемент контроля у личности [7]. Получается замкнутый круг, согласие в нынешнем виде не справляется, но без него индивид останется вовсе безоружным перед сбором данных.

Проведенный анализ показывает, что решение проблемы видится не в отказе от концепции согласия, а в ее перезагрузке и комплексном усилении. Необходимо повышать стандарт осознанности, упрощая коммуникацию и стандартизируя объяснения [7]. Требуется обеспечить добровольность на деле, не допуская принуждения человека под угрозой исключения из социально значимых сервисов. Контроль над соблюдением условий согласия должен усилиться, за этим нужен строгий надзор и ответственность [8]. Сам подход к защите данных должен становиться более проактивным, что ограничивает сбор и использование данных до минимума и снижает зависимость от согласия как панацеи. Крупные цифровые игроки должны осознавать свою обязанность не эксплуатировать информационную неграмотность пользователей, а напротив, помогать им. Институциональные инновации, от комиссий по этике данных до коллективных механизмов управления, могут дополнить институт согласия, подстраховывая его там, где индивид объективно слаб. В конечном счете, защита персональных данных – это ответственность не только самих граждан, но и государства, и бизнеса, и гражданского общества. Только совместными усилиями можно сделать так, чтобы в цифровом мире высокий уровень технологий не означал низкий уровень приватности. Как метко сформулировано в решении немецкого суда 1983 года, свободное развитие личности в условиях современного сбора данных требует защиты индивида от неограниченного использования его персональной информации, а значит гарантии за самим индивидом властных полномочий определять судьбу своих данных. В сущности, речь идет о том, каким будет будущее цифрового общества, либо основанным на сознательном согласии и доверии, либо на скрытых манипуляциях и подчинении. Ответ на этот вопрос во многом зависит от того, сможем ли мы наполнить институт согласия реальным содержанием.

Список использованных источников:

1. Warren, S. D. The Right to Privacy / S. D. Warren, L. D. Brandeis // Harvard Law Review. – 1890. – Vol. 4, № 5. – P. 193-220.

2. Westin, A. F. Privacy and Freedom / A. F. Westin. – 1st ed. – New York : Atheneum, 1967. – 487 p.

3. Charter of Fundamental Rights of the European Union // Official Journal of the European Communities. – 2000. – 18 December. – C 364. – P. 1-22.

4. Конституция Республики Беларусь : с изм. и доп., принятыми на респ. референдумах 24 нояб. 1996 г., 17 окт. 2004 г. и 27 февр. 2022 г. – Минск : Нац. центр правовой информ. Респ. Беларусь, 2024. – 109 с.

5. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 07.07.2025) «О персональных данных» // Собрание законодательства Российской Федерации. – 2006. – № 31 (1 ч.). – Ст. 3451.

6. McDonald, A. M. The Cost of Reading Privacy Policies / A. M. McDonald, L. F. Cranor // I/S: A Journal of Law and Policy for the Information Society. – 2008. – Vol. 4, № 3. – P. 543-568.

7. Solove, D. J. Introduction: Privacy Self-Management and the Consent Dilemma / D. J. Solove // Harvard Law Review. – 2013. – Vol. 126, № 7. – P. 1880-1903.

8. Lynskey, O. The Foundations of EU Data Protection Law / O. Lynskey. – 1st ed. – Oxford : Oxford University Press, 2015. – 307 p.

9. Zuboff, S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power / S. Zuboff. – 1st ed. – New York : PublicAffairs, 2019. – 704 p.