УДК 347.9 (476)

НЕКОТОРЫЕ ВЫЗОВЫ ПРАВОВОМУ РЕГУЛИРОВАНИЮ ПРАВ ЧЕЛОВЕКА В ЭПОХУ ЦИФРОВОЙ ЭКОНОМИКИ

А. А. Шафалович
Белорусский государственный экономический университет

Аннотация

Данная статья выявляет потенциальные вызовы правовому регулированию в области прав человека, которые в случае их игнорирования могут привести к утрате человеком статуса субъекта права прав человека и цифровому рабству.

Ключевые слова: права человека, персональные данные, электронное государство, цифровая экономика, цифровизация, цифровые права, киберпреступления, цифровое неравенство, искусственный интеллект, перспективное правовое регулирование.

С одной стороны, использование цифровых технологий позволяет получить принципиально новые возможности для оптимизации защиты фундаментальных прав и свобод человека и гражданина.

С другой стороны, инновационные проекты, как драйверы экономического роста и развития, одновременно являются и факторами нарушения устойчивости сложившейся системы, заключая в себе определенные вызовы, риски и угрозы для прав человека. Назовем некоторые из вызовов.

1) Возможно распространение дискриминации по информационному признаку [1, с. 22], производной от невысокого уровня информатизации населения в целом, недостаточного числа пользователей электронными услугами (и государственных служащих в том числе). Проблема доступа к ИКТ и степени владения технологиями со стороны населения в настоящее время обозначена как проблема «цифрового неравенства», «глобальный цифровой разрыв», «цифровая бездна», разделяющая общество на две части: тех, кто бесконтрольно имеет возможность пользоваться высокими технологиями, и тех, кому они по разным причинам недоступны. Как и социальное, цифровое неравенство способно существенно дестабилизировать нормальное функционирование общественного процесса и государственного управления.

Одним из аспектов цифрового неравенства является киборгизация. Растущее число людей, которые используют различные киберкомплектующие, чтобы повысить качество своей жизни и расширить возможности, в том числе когнитивные. Речь идет о гаджетах, которые глубоко взаимодействуют с организмом человека, например, имплантах с микроэлектроникой, разного рода киберпротезах и бионических протезах. В результате массовой киборгизации может реализовываться не внушающее оптимизма кибертехнократическое общество [2, с. 115–120]. Возникает противоречие между виртуальным пространством потоков для избранных и реальным пространством жизни для

остальных, в перспективе грозящий обществу катастрофическими последствиями.

2) В условиях развития электронного государства увеличение количества электронных услуг и пользователей государственных электронных услуг происходит на фоне снижения практически всех параметров «качества жизни» [3, с. 245].

В рамках постиндустриального общества информационное преимущество является важной социальной силой, способствующей перераспределению экономических, социальных и политических ресурсов. Вместе с тем информационное неравенство ведет и к социальному неравенству. В контексте электронного государства в «отечественной модели цифровизации государственного управления» акцент смещается на предоставление государственных услуг в электронной форме, при этом рост благосостояния людей (который все-таки определяется через понятия, связанные с материальными благами) замещается их доступом к электронным государственным услугам. Новые цифровые технологии в нашем случае не помогают решению социально-экономических проблем [3, с. 250].

3) Новейшие технологии могут быть использованы не только на пользу человечеству, но и в праворазрушительных, криминальных целях, если попали «не в те руки». По мере развития информационных процессов растет уязвимость информации. Вследствие возрастающей степени информатизации общества и диджитализации протекающих в нем процессов возникает зависимость от уровня защищенности применяемых ИКТ. В ходе технического прогресса все более актуальной становится проблема защиты конфиденциальной информации, хранящейся в корпоративных информационных сетях, в том числе государственного уровня. При этом следует отметить, что в данной области факторы риска могут носить как естественный и непреднамеренный характер (отключение питания сервера, ошибка в программном коде), так и являться целенаправленными и умышленными (спланированная кибератака). В научной литературе говорят о новой, третьей фазе законодательства о защите персональных данных [4, с. 137].

Наблюдается тенденция устойчивого роста компьютерной преступности, грозящей перерасти в серьезную проблему. При этом вытекая из IT-сферы, данные факторы влекут за собой далеко идущие последствия в политической, военной и, безусловно, экономической сфере. Так, эксперты предупреждают, что при применении соответствующей технологии в сфере гражданско-правовых отношений теоретически существует вероятность осуществления так называемой «атаки 51 %», когда группа участников сети сконцентрирует в своих руках 51 % вычислительных мощностей и сможет таким образом начать действовать в своих интересах, подтверждая только выгодные для себя транзакции [5].

4) Актуальной проблемой взаимоотношений человека и власти в цифровом обществе является определение возможных ограничений цифровых прав законом, в том числе допустимых пределов контроля информационной

среды со стороны правоохранительных служб с целью обеспечения эффективной защиты общества от киберпреступлений [5].

«Анализ «больших данных» («BigData») неизбежно затронет большинство людей, так как их поведение, перемещение, реализация желаний станут объектом постоянного наблюдения и системного анализа, что существенным образом ограничит пределы их частной жизни» [6, с. 72].

Все это свидетельствует о необходимости поиска в законодательном регулировании оптимального правового компромисса между возможностью доступа правоохранительных служб к компьютерной информации и правом граждан на ее конфиденциальность.

Как всегда, сложным будет отыскание баланса между регулятивными и охранительными нормами. С одной стороны, государство не должно оставлять человека в сети Интернет один на один с преступными посягательствами на его права, законные интересы и имущество. Но, с другой стороны, применяемые технологии противодействия преступности не должны превращаться в чрезмерные ограничения, посягая на саму суть конституционного права на информацию и находящейся под его защитой свободы поведения человека в интернете. М. А. Грачева отмечает, что «систематический сбор сведений секретными службами представляет собой вмешательство в частную жизнь, даже если эти сведения получены в общественных местах и если содержат информацию исключительно о профессиональной или общественной деятельности лица. Те же действия, осуществляемые посредством применения GPS-технологий, и хранение данных о местонахождении лица и его передвижениях также представляют собой вмешательство в частную жизнь» [7, с. 137]. В этом отношении баланс между частным и публичным интересами призваны находить суды.

Если на массовом уровне защита частной жизни ослабевает под натиском цифровых технологий, то на индивидуальном уровне тенденция кажется обратной — праву на защиту персональных данных уделяется все большее внимание в связи с использованием цифровых технологий.

5) Информатизация может стать источником ряда серьезных психических проблем. Психологические риски связаны прежде всего с т.н. «электронным вторжением» в подсознание людей, которое можно представить как электронную сетевую несвободу. «Виртуализм» проявляется в отстранении личности от реальных жизненных впечатлений и проблем и уходе в виртуальный мир. По оценкам психологов, только 15–20 % населения способны критически усваивать информацию, в то время как 75 % людей обладают повышенной внушаемостью. Вследствие этого применение современных средств и способов информационного воздействия на человека обеспечивает управляемость обществом в соответствии с определенными целями.

Таким образом, в целях обеспечения прогресса в праве правовое регулирование потребностей цифровой экономики должно осуществляться лишь с учетом примата фундаментальных прав человека. В связи с чем правовая наука призвана использовать перспективный тип правового регулирования и незамедлительно реагировать на вызовы в области прав человека, связанные с

угрозой цифрового неравенства, снижения параметров «качества жизни», риском попадания технологий «не в те руки», с риском несоразмерного ограничения цифровых прав законом и с рисками для здоровья человеческой психики.

Список использованных источников:

1. Комаров, С. А. Переходное электронное государство в условиях функционирования информационной (кибернетической) цивилизации: теоретико-правовой анализ / С. А. Комаров, С. М. Воробьев // Вестник Московского государственного областного университета. – Сер. Юриспруденция. – 2019. – № 1. – С. 17–27.
2. Шафалович, А. А. Правовое обеспечение развития электронного государства : учеб. пособие / А. А. Шафалович. – Минск: Амалфея, 2021. – 207 с.
3. Шаулова, Т. В. Цифровизация и эффективность государственного управления / Т. В. Шаулова // Науч. тр. Северо-Западного института управления РАНХиГС. – 2019. – Т. 10. – № 2. – С. 243–252.
4. Талапина, Э. В. Эволюция прав человека в цифровую эпоху / Э. В. Талапина // Труды Института государства и права РАН. – 2019. – Т. 14. – № 3. – С. 122–146.
5. Зорькин, В. Д. Право в цифровом мире. Размышление на полях Петербургского международного юридического форума [Электронный ресурс] // Российская газета. 2018. Столичный выпуск № 7578 (115). 29 мая. – Режим доступа : https://rg.ru/2018/05/29/zorkin-zadacha-gosudarstva-priznavat-i-zashchishchat-cifrovye-prava-grazhdan.html. – Дата доступа : 21.09.2022.
6. Фатьянов, А. А. Актуальные проблемы правового регулирования в области развития цифровой экономики / А. А. Фатьянов // Ученые труды Российской академии адвокатуры и нотариата. – 2018. – № 3(50). – С. 71–77.
7. Грачева, М. А. Право человека на уважение частной жизни и его защита в Европейском суде по правам человека / М. А. Грачева // Международный журнал конституционного и государственного права. – 2017. – № 1. – С. 135–140.