АКТУАЛЬНЫЕ ПРОБЛЕМЫ ЦИФРОВИЗАЦИИ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

БЕЗДОЛЬНЫЙ
Олег Сергеевич

студент 4 курса Института публичного права и управления Университета имени О.Е. Кутафина (МГЮА)

bezdolnyoleg2@gmail.com

Аннотация. *В данной статье рассматривается проблематика защиты прав и законных интересов граждан в период перехода государства к системам цифрового управления, защита персональной информации при создании масштабных баз данных, а также анализ угроз, которые существуют на данный момент и которым стоит уделить особое внимание.*
Ключевые слова: *государственное управление, технологии, персональные данные, информационные системы.*

Для цитирования: Бездольный О.С. Актуальные проблемы цифровизации государственного управления // Сфера права. 2020. № 2. С. 10–11.

Новейшие технологии, которые с каждым годом проникают в жизнь обычных людей все сильнее, не могли обойти стороной и вопросы, связанные с государственным управлением. Ведь, действительно, благодаря достижениям научно-технического прогресса уже сейчас граждане России могут получить информацию из государственных органов даже не выходя из дома, а во многие органы власти уже сейчас внедряются системы, позволяющие выполнять задачи, возложенные на них, гораздо быстрее и качественнее. Например, система «АСК НДС-3»[10], помогающая налоговым органам выявлять в автоматическом режиме подозрительные сделки, которые предприниматели могут заключать со своими контрагентами через подставные компании для ухода от уплаты НДС, таким образом снижая количество недополученных доходов в бюджеты разных уровней и повышая налоговую грамотность среди предпринимателей.

Также нельзя не отметить, что благодаря внедрению информационных технологий в правоохранительные органы значительно повысилась раскрываемость преступлений, в том числе и по преступлением небольшой тяжести, например, кража велосипедов или колясок. Ведь если раньше правоохранительные органы с большой неохотой брались за расследование таких преступлений, то теперь, например, благодаря системам распознавания лиц, которые установлены во многих общественных местах Москвы, таких мелких преступников стали ловить значительно чаще[11].

Нельзя не отметить и достижения в области создания электронных баз данных. Так, уже в 2020 году в России в тестовом режиме на территории Москвы будут запущены электронные паспорта, которые по сути будут представлять собой сведения, которые необходимы гражданину, например, для устройства на работу или для обращения в государственные органы: СНИЛС, ИНН, паспортные данные и пр.[12] Потенциально такой паспорт способен избавить граждан от необходимости иметь при себе большое количество

[10] Автоматизированная система контроля за возмещением НДС.

[11] Раскрываемость преступлений в Москве находится на самом высоком уровне за последние 10 лет // URL: https://www.mos.ru/mayor/themes/10299/5350050/ (дата обращения: 06.10.2019).

[12] Считайте, завидуйте. Кабмин решил ускорить переход на электронные паспорта // URL: https://rg.ru/2019/07/17/pravitelstvo-reshilo-uskorit-perehod-na-elektronnye-pasporta.html (дата обращения: 06.10.2019).

иных документов. Объем такой информации требует затрат большого количества ресурсов, поэтому, в целом, очевидно, что государственные органы сейчас крайне заинтересованы в возможностях, которые могут предоставить современные технологии, включая такие прогрессивные отрасли IT-индустрии, как Big Data, то есть структурированные и неструктурированные данные огромных объёмов и значительного многообразия, эффективно обрабатываемые горизонтально масштабируемыми программными инструментами и нейросетями, которые уже сейчас способны совершить переворот во многих отраслях индустрии.

Однако развитие технологий в сфере государственного управления может нести и риски, в первую очередь, для граждан. Уже сейчас в сети Интернет можно купить информацию из баз данных различных органов государственной власти, которые не должны быть доступны посторонним лицам. При этом злоумышленники даже не пытаются каким-либо образом скрыть свою нелегальную деятельность, продавая информацию прямо через поисковые системы, чувствуя свою безнаказанность. Таким образом, даже сейчас персональные данные граждан не всегда хорошо защищены от всевозможных посягательств. Но что будет, когда на территории всей Российской Федерации будет введена система распознавания лиц и злоумышленники смогут получить доступ к ней? Они смогут отслеживать перемещения лиц, не только нарушая их право на неприкосновенность личной жизни, но и планировать преступления, изучая распорядок дня или маршрут потенциальной жертвы.

Вторая проблема — это отсутствие развитого законодательства в области защиты персональных данных. Действующий сейчас Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»[13] не выполняет в полной мере тех функций, которые на него возложены. Очевидно, что гарантированное данным законом в ст. 7 право на соблюдение конфиденциальности субъекта персональных данных не соблюдается, и персональная информация без каких-либо проблем попадает в руки к третьим лицам, причем не только от недобросовестных работников коммерческих структур, но и от сотрудников государственных структур. На мой взгляд, решение данной проблемы лежит зависит не только от законодательного регулирования, хотя и от нем в том числе, но и от правосознания операторов персональных данных. Ведь стоит понимать, что базы данных, ушедшие в сеть, способны не только быть использованы операторами call-центров для назойливых звонков потенциальным клиентам, но и самыми настоящими преступниками для гораздо более опасных действий.

Не стоит также забывать и об уязвимости информационных систем, которые могут быть подвержены хакерским атакам извне, способным обрушить всю цифровую инфраструктуру, сбои в работе из-за которых могут значительно затруднить работу сотрудников государственных органов, и о возможности попадания информации о функционировании и технических особенностях информационных систем к широкому кругу людей, в том числе к злоумышленникам, которые могут воспользоваться этими данными для корыстных целей. Примером такой «утечки» может послужить раскрытие особенностей функционирования СОРМ[14], произошедшее по вине сотрудников компании Nokia, осуществлявших обслуживание данной системы.

Однако стоит понимать, что сейчас за цифровыми технологиями будущее, и для возможности дальнейшего совершенствования государственного и муниципального аппарата обойтись без них никак нельзя. Но все-таки не стоит забывать и о вызовах, которые эти технологии способны бросить нашему обществу и государству.

---

[13] СЗ РФ. 2006. № 31. Ст. 3451.

[14] Система технических средств для обеспечения функций оперативно-разыскных мероприятий. См.: Telecommunications Breakdown: How Russian Telco Infrastructure was Exposed // URL: https://www.upguard.com/breaches/mts-nokia-telecom-inventory-data-exposure (дата обращения 06.10.2019).