

Н. В. Пушко

доцент кафедры правовых дисциплин
факультета повышения квалификации
и переподготовки кадров
Могилевского института МВД,
кандидат экономических наук, доцент

А. О. Маров

курсант 2-го курса факультета милиции
Могилевского института МВД

АКТУАЛЬНЫЕ АСПЕКТЫ ПРАВА НА ПРИВАТНОСТЬ В ЭПОХУ ЦИФРОВИЗАЦИИ ОБЩЕСТВА

CURRENT ASPECTS OF THE RIGHT TO PRIVACY IN THE ERA OF DIGITALIZATION OF SOCIETY

Аннотация. В статье проанализировано право на приватность как совокупность мер, которые направлены на защиту личных данных и частной жизни от вмешательства иных лиц. Особое внимание уделено рассмотрению защиты информационной приватности как одного из основных элементов права на приватность в целом в современном цифровизированном обществе, а также правовой охране личного информационного пространства.

Ключевые слова: право на приватность, цифровизация, информационное пространство, защита, персональные данные, личность.

Annotation. The article analyzes the right to privacy as a set of measures aimed at protecting personal data and private life from interference by other persons. Particular attention is paid to the consideration of the protection of information privacy as one of the main elements of the right to privacy in general in a modern digitalized society, as well as the legal protection of personal information space.

Keywords: right to privacy, digitalization, information space, protection, personal data, personality.

В настоящее время право на приватность как совокупность мер, которые направлены на защиту личных данных и частной жизни от вмешательства иных лиц, приобретает важнейшее значение. Рассматривая ретроспективу понятия права на приватность, нельзя не упомянуть работу С. Уоррена и Л. Брендайса «Право быть оставленным в покое» (1890), в которой авторы впервые отстаивали право индивида на возможность выбрать уединение от других людей, на защиту

личности от постоянного общественного контроля [1]. В ранний советский период данное понятие прочно ассоциировалось с буржуазными ценностями, и поэтому приоритетным было коллективное право в ущерб личному, и только в Конституции СССР 1936 г. право на неприкосновенность личности было закреплено нормативно [2]. Во второй половине XX в. стало понятно, что право на приватность должно быть закреплено в международных правовых нормах, итогом чего стала ст. 17 Международного пакта о гражданских и политических правах (1966) [3] и ст. 12 Всеобщей декларации прав человека (1948), в которой было сформулировано следующее: «Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств» [4].

В действующей Конституции Республики Беларусь 1994 г. государство выступает гарантом признания и защиты этого права [5]. В частности, ст. 28 Основного Закона гласит, что каждый имеет право на защиту от незаконного вмешательства в его частную жизнь, в том числе от посягательства на тайну его корреспонденции, телефонных и иных сообщений, на его честь и достоинство. Также охрана права на приватность предусмотрена и в ст. 151 Гражданского кодекса Республики Беларусь [6], в которой предусмотрены права на защиту достоинства личности, чести и доброго имени, деловой репутации, неприкосновенности частной жизни, личной и семейной тайны и др.

В связи с тем, что многие информационные, технологические, экономические и социальные процессы уже нельзя себе представить без применения цифровых технологий, защита права лица на приватность, в том числе защита его персональных данных в интернет-среде, уже невозможна без правового регулирования со стороны государства. В современном цифровизированном обществе для защиты информационной приватности как одного из основных элементов права на приватность в целом принят Закон Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» [7], который установил, что к защищаемым сведениям можно отнести практически любую информацию о физическом лице. То, что наше государство придает праву на приватность, в том числе праву на защиту персональных данных, такое большое значение, подтверждается тем, что по Указу Президента Республики Беларусь от 28 октября 2021 г. № 422 «О мерах по совершенствованию защиты персональных данных» [8] 15 ноября 2021 г.

создан Национальный центр защиты персональных данных, учредителем которого является Оперативно-аналитический центр при Президенте Республики Беларусь.

Обобщая мнения различных исследователей в области защиты права на цифровую приватность, к основным нарушениям такового можно отнести:

1) незаконный сбор данных (например, использование скрытых камер или прослушивающих устройств для наблюдения за человеком без его ведома);

2) распространение личной информации через публикацию или передачу персональных данных (например, сведений об адресе, телефоне) без согласия человека;

3) киберпреследование — мониторинг активности человека в Интернете, взлом аккаунтов, использование личных данных для шантажа или угроз;

4) несанкционированный доступ к данным (взлом базы данных компании для получения информации о клиентах или сотрудниках или взлом систем, через которые проходит оборот денег, с угрозой их потери для пользователя);

5) нарушение конфиденциальности переписки (чтение чужих писем, сообщений или прослушивание телефонных разговоров, просмотр фотографий или видео без разрешения самого пользователя);

6) использование данных в коммерческих целях (продажа личной информации третьим лицам, рекламным компаниям без согласия лица);

7) публикация фотографий или видео без согласия человека и др.

Учитывая высокую активность современных правонарушителей в цифровой среде, вопрос обеспечения защиты данных благ становится особенно актуальным. Охрана права на информационную приватность предполагает и использование особых способов, направленных на обеспечение ее безопасности: технологические меры (например, шифрование данных при передаче или хранении); политика конфиденциальности (все компании обязаны предоставлять пользователю информацию о том, как они собирают, используют и защищают персональные данные); самозащита данных (к примеру, установка двухфакторной аутентификации, регулярные проверки на вредоносные программы и др.); осведомленность (например, через обучение пользователей правильному использованию цифровой средой). При этом базовыми мерами являются защита на законодательном уровне, а также распространение информации о необходимости сохранения своей информационной приватности через социальную среду.

Между тем проблема информационной безопасности связана не только с охраной личного информационного пространства индивида, но и с выполнением государством задач по защите граждан от киберпреступности. При этом главный вопрос заключается в балансе безопасности (в том числе и путем добровольного отказа граждан от части их приватности) и свободы личности. В связи с тем, что в цифровую эпоху каждое действие в сети Интернет оставляет свои цифровые следы, а государство, в свою очередь, старается максимально обезопасить граждан от преступных онлайн-посягательств, многие пользователи считают, что оно слишком жестко ограничивает права интернет-абонентов, не беря во внимание то, что хакеры используют все скрытые уязвимости для того, чтобы поставить под угрозу их персональную информационную безопасность. Преступники применяют различные мошеннические схемы для получения финансовой выгоды от взлома персональных данных: фишинг, вредоносные программы, социальная инженерия (использование выдуманных легенд, психологических приемов и др.), использование поисковых систем в сети Интернет, в том числе получение информации в открытых источниках, что особенно актуально для тех пользователей, которые не заботятся о своей цифровой гигиене, и многие другие.

В итоге интернет-пользователь, с одной стороны, жалуется на чрезмерный контроль цифрового пространства государством, а с другой стороны, сталкиваясь со все более возрастающей угрозой со стороны хакеров, мошенников, обращается за защитой своих персональных данных к тому же государству, что приводит к затруднениям в достижении баланса между безопасностью и личной свободой в цифровой сфере. При этом сам такой баланс не статичен, а постоянно находится в динамике в связи с тем, что каждый день появляются как новые угрозы, так и новые методы и меры борьбы с ними. Поэтому государству необходимо соблюдать некоторые условия для поддержания вышеназванного баланса, такие как прозрачность (нужно четко объяснять гражданам необходимость сбора, хранения, передачи и использования данных); сотрудничество (законодательные усилия в этой области позволяют сократить количество экстерриториальных цифровых преступлений) и осведомленность (напоминание о самозащите играет значительную роль в борьбе с киберпреступностью).

Таким образом, цифровые технологии, открывая широкие возможности для сбора, анализа и использования персональных данных, не только повышают эффективность оказания государственных услуг и продвижения бизнеса, но и создают угрозы для информационной

безопасности, поскольку утечки таких данных и манипуляции на основе алгоритмов подрывают доверие людей к цифровым системам. Для достижения баланса в части соотношения права на приватность и безопасность пользования цифровой средой необходимы усилия как со стороны государства, так и со стороны каждого индивида. В частности, в рамках национального законодательства потребуется комплексный подход к определению основных видов мошенничеств, связанных с использованием персональных данных, усовершенствование идентификации цифровых преступлений, что особенно актуально в контексте противодействия отмыванию нелегальных доходов. В свою очередь, со стороны каждого человека необходимы усилия по закреплению моделей поведения, которые направлены на бережное и осторожное обращение со своими личными данными в сети Интернет, на формирование культуры обращения с такой информацией. Из этого следует, что достижение баланса между безопасностью и свободой требует совместных усилий всех участников цифрового пространства: государства, бизнеса, технологических компаний и самих пользователей. Только так можно создать устойчивую систему, где технологии служат людям, а не угрожают их правам и свободам.

Список основных источников

1. Хужокова, И. М. Конституционное право человека и гражданина на неприкосновенность частной жизни в Российской Федерации : автореф. дис. ... канд. юрид. наук : 12.00.02 / Хужокова Ирина Михайловна ; Поволж. акад. гос. службы им. П. А. Столыпина. – Саратов, 2007. – 27 с.
2. Конституция СССР 1936 г. // ГАРАНТ.РУ : информ.-правовой портал. – URL: <https://constitution.garant.ru/history/ussr-rsfsr/1936/> (дата обращения: 03.06.2025).
3. Международный пакт о гражданских и политических правах : принят резолюцией 2200 А (XXI) Генер. Ассамблеи ООН от 16 дек. 1966 г. // Организация Объединенных Наций. – URL: https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml (дата обращения: 03.06.2025).
4. Всеобщая декларация прав человека : принята резолюцией 217 А (III) Генер. Ассамблеи ООН от 10 дек. 1948 г. // Организация Объединенных Наций. – URL: https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml (дата обращения: 03.06.2025).
5. Конституция Республики Беларусь 1994 года : с изм. и доп., принятыми на респ. референдумах 24 нояб. 1996 г., 17 окт. 2004 г. и 27 февр. 2022 г. // ЭТАЛОН : информ.-поисковая система (дата обращения: 03.06.2025).
6. Гражданский кодекс Республики Беларусь : 7 дек. 1998 г., № 218-3 : принят Палатой представителей 28 окт. 1998 г. : одобр. Советом Респ. 19 нояб. 1998 г. : в ред. от 17 февр. 2025 г. № 62-3 // ЭТАЛОН : информ.-поисковая система (дата обращения: 03.06.2025).

7. О защите персональных данных : Закон Респ. Беларусь от 7 мая 2021 г. № 99-З : в ред. от 1 июня 2022 г. № 175-З // ЭТАЛОН : информ.-поисковая система (дата обращения: 03.06.2025).

8. О мерах по совершенствованию защиты персональных данных : Указ Президента Респ. Беларусь от 28 окт. 2021 г. № 422 : в ред. от 7 авг. 2025 г. № 300 // ЭТАЛОН : информ.-поисковая система (дата обращения: 03.06.2025).

УДК 343.98

Д. А. Свиридов
начальник кафедры уголовного права,
уголовного процесса и криминалистики
Могилевского института МВД

К ВОПРОСУ О ПОНЯТИИ КОРРУПЦИОННЫХ РИСКОВ В КОНТЕКСТЕ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ ДОЛЖНОСТНЫХ ПРЕСТУПЛЕНИЙ

ON THE QUESTION OF THE CONCEPT OF CORRUPTION RISKS IN THE CONTEXT OF FORENSICAL CHARACTERISTICS OF OFFICIAL CRIMES

Аннотация. Центральной проблемой, рассматриваемой в данной статье, выступают такие категории, как коррупционные риски и расследование коррупционных и должностных преступлений. Делается акцент на понимании коррупционных рисков и необходимости разработки эффективных частных методик выявления и расследования указанных преступлений. Также определяется центральный элемент частной методики расследования коррупционных и должностных преступлений — криминалистическая характеристика. Рассматриваются наиболее значимые элементы криминалистической характеристики коррупционных и должностных преступлений.

Ключевые слова: коррупционный риск, должностное преступление, расследование, преступление, криминалистическая характеристика.

Annotation. The central problem of this article is such categories as corruption risks and investigation of corruption and official crimes. The emphasis is placed on understanding corruption risks and the need to develop effective private methods for identifying and investigating such crimes. The central element of the private method for investigating corruption and official crimes is also determined — forensic characteristics. The most significant elements of the forensic characteristics of corruption and official crimes are considered.