почте и дистанционного электронного голосования по определению однозначно не гарантирует от криминализации отмеченных двух новых технологий голосования [1]. Резюмируя изложенное, по нашему мнению представляется обоснованным заметить следующее: во-первых, процесс дальнейшего демократического устройства современного общества неотделим от процесса возникновения новых, более изощренных и техногенных по своему содержанию форм и способов электоральной преступности, посягающей на основополагающие права граждан по их непосредственному участию в политической жизни страны посредством реализации своего активного и пассивного избирательного права; во-вторых, исследование особенностей цифровой преступности и ее деструктивного воздействия на основы российского конституционализма, предопределяющего безусловность защиты избирательных прав граждан, может быть отнесено к важному и перспективному направлению исследования для отечественной криминологии; в-третьих, необходимость процесса технического переоснащения современного избирательного процесса в формате дальнейшей модернизации национальной избирательной системы неотделима от качества и своевременности правового регулирования всех его этапов, с учетом феномена дигитализации общественного сознания избирательского корпуса, цифровых потребностей и запросов общества, а также необходимости создания более прочных и адекватных барьеров на пути распространения новых вариаций цифровой преступности.

1. Федеральный закон от 23 мая 2020 г. № 154-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // Российская газета, 25 мая 2020. - № 110.
2. Гилинский Я.И. Криминология: теория, история, эмпирическая база, социальный контроль / Я.И. Гилинский. - СПб: Алеф-Пресс, 2014. - 574 с.
3. Дюркгейм Э. Норма и патология / Э. Дюркгейм; ред. проф. А.С. Никифорова // Социология преступности (современные буржуазные теории): сборник статей. - М.: Прогресс, 1966. - С. 39-45.
4. Иванов А.А., Шагиева Р.В. Основной вопрос криминологии: взгляд сквозь призму истории / А.А. Иванов, Р.В. Шагиева // Вестник Московского государственного областного университета. - 2017. - № 4. - С. 139-155.
5. Клейменов М.П. Криминологическое законодательство и криминологическое право в России / М.П. Клейменов // Lex Russia. - 2018. - № 2 (135). - С. 148-159.
6. Мертон Р. К. Социальная структура и аномия / Р.К. Мертон; ред. проф. А.С. Никифорова // Социология преступности (современные буржуазные теории): сборник статей: - М.: Прогресс, 1966. - С. 299-313.
7. Николаев А.М. Пределы криминализации деяний с учетом характера учета и степени их общественной опасности (истoki и перспективы формирования новой теории) / А.М. Николаев // Пробелы в российском законодательстве. - 2008. - № 1. - С. 322-324.
8. Решение Чертановского районного суда по делу № 02а-0296/2019. - URL: <https://www.mos-gorsud.ru> (дата обращения: 17 мая 2020)
9. Цифру готовят к ответу. Электронное голосование в Москве станет предметом разбирательства в суде. - URL: <https://www.kommersant.ru/doc/4096569> (дата обращения: 19 мая 2020)
10. Шестаков Д.А. Криминологическое законодательство и право противодействия преступности / Д.А. Шестаков // Криминология вчера, сегодня и завтра. - 2013. - № 1 (28). - С. 48-49.

Чимаров С.Ю.

Правовые основы запрета и ограничения использования сети «Интернет» в системе МВД и Вооруженных Силах России: сравнительный анализ

*Санкт-Петербургский университет МВД России
(Россия, Санкт-Петербург)*

doi: 10.18411/lj-06-2020-387

idsp: ljjournal-06-2020-387

Аннотация

В статье представлен анализ нормативно-правового регулирования действующих ограничений и запретов на использование сетевой коммуникации в

системе МВД и Вооруженных Сил России. Проводя сравнительно-правовой анализ отмеченной области, автор акцентирует внимание на более жесткой регламентации действий военнослужащих в сетевом пространстве и более строгие для них запреты во время несения службы в части применения соответствующих электронных устройств.

Ключевые слова: органы внутренних дел, сотрудники органов внутренних дел, военнослужащие, цифровая бдительность, цифровой след, цифровая тень, сетевое пространство, киберпреступность, сетевые угрозы.

Abstract

The article presents an analysis of the legal regulation of existing restrictions and prohibitions on the use of network communication in the system of the Ministry of internal Affairs and the Armed Forces of Russia. Conducting a comparative legal analysis of this area, the author focuses on stricter regulation of actions of military personnel in the network space and stricter prohibitions for them during their service in terms of the use of appropriate electronic devices.

Keywords: law enforcement agencies, law enforcement officers, military personnel, digital vigilance, digital footprint, digital shadow, network space, cybercrime, network threats.

Фактор форсированного интегрирования в систему межинституциональной и межличностной коммуникации информационных технологий и определения сети «Интернет» к разряд неизбежного атрибута социального взаимодействия предопределяет демонстрацию не только очевидных преимуществ новых технологий, но и способствует масштабному проявлению угрозы суверенитету государства, нанесению ущерба его национальной безопасности, появлению новых видов преступности и цифровой форме нарушения прав и свобод человека. Наряду с отмеченным, следует обратить внимание на сопряженность сетевых угроз с фактором негативного воздействия на поведенческие установки личности сотрудника органов внутренних дел или военнослужащего, обязанных соблюдать каноны цифровой бдительности. Указанный тезис подтверждается выводом Р. Чесни и Д. К. Цитрон, обративших внимание на то, что современная сетевая информационная среда токсичным образом взаимодействует с нашим когнитивным искажением [6, p. 1724]. В данном случае, термин «когнитивное искажение» (англ. «cognitive biases») означает переход мозговой деятельности от логического мышления в область заблуждений (англ. «which is where the brain deviates from logical thought into fallacy»). Серьезную опасность в плане утечки секретной и иной служебной информации, циркулирующей в системе МВД и в Вооруженных Силах России можно проиллюстрировать цитатой из доклада ЦРУ: «Стремительное увеличение объемов информации из открытых источников, ставшее результатом подключения к Интернету все более умных устройств, является, пожалуй, самым ярким незасекреченный примером перспектив и опасностей новых технологий» [5].

Изложенное выше и ряд иных обстоятельств, обусловленных особенностями деятельности сотрудников органов внутренних дел и военнослужащих, предопределяет целесообразность запрета и ограничений использования сети «Интернет» в системе МВД и Вооруженных Силах России. В соответствии со ст. 14 «Ограничения, обязанности и запреты, связанные со службой в органах внутренних дел» Федерального закона от 30 ноября 2011 г. № 342-ФЗ, для сотрудников ОВД не предусматриваются ограничения и запреты в части использования сетью «Интернет» [1]. Вместе с тем, Методические рекомендации МВД России от 13 марта 2020 г. № 1/2704 конкретизируют правовые пределы компетенции сотрудников в части

использования сети «Интернет» [4]. Уточняя обоснование принятия Методических рекомендаций с учетом возрастания масштаба киберпреступности, воздействующей в том числе на область частной жизни сотрудников, данный документ содержит два раздела: 1) актуальные угрозы безопасности персональным данным сотрудников органов внутренних дел и их близких; 2) способы противодействия угрозам безопасности персональным данным сотрудников органов внутренних дел и их близких. В Методических рекомендациях представлена общая характеристика возможного цифрового присутствия сотрудников, а также определяется содержание цифрового следа или «данных, самостоятельно передаваемых в цифровую среду» и цифровой тени или «информации, создаваемой о людях автоматически посредством действий и устройств третьих лиц» [4, с. 7]. Детализация регламентации использования сети «Интернет» и иных средств онлайн-коммуникации для сотрудников органов внутренних дел, включая запреты и ограничения, закреплена в ряде ведомственных нормативных правовых актов. В Вооруженных Силах России область запретов и ограничений в отмеченной сфере регламентируется в соответствии с Указом Президента Российской Федерации от 06 мая 2020 г. № 308 [3], согласно которому внесены правовые новеллы в Дисциплинарный устав Вооруженных Сил России (далее - ДУ ВС РФ) и Устав гарнизонной и караульной служб Вооруженных Сил России (далее - УГиКС ВС РФ) [2]. С учетом данных изменений, в п. 1 приложения № 7 ДУ ВС РФ расширен перечень грубых дисциплинарных проступков военнослужащих, к которым отнесены:

а) нарушение запрета предоставлять СМИ либо с использованием сети «Интернет» распространять или предоставлять: информацию, позволяющую определить принадлежность или предназначение военнослужащих к Вооруженным Силам России, другим войскам, воинским формированиям и органам; информацию о других военнослужащих, гражданах, уволенных с военной службы, членах их семей или их родителях, в том числе информацию, позволяющую определить место нахождения указанных лиц в определенный период другим лицам; информацию о своей деятельности или деятельности других военнослужащих и граждан, уволенных с военной службы, связанной с исполнением обязанностей военной службы; информацию о деятельности органов военного управления или органов управления другими войсками, воинскими формированиями и органами, о деятельности объединений, соединений, воинских частей и иных организаций, входящих в состав Вооруженных Сил России или других войск, воинских формирований и органов, о деятельности подразделений указанных органов военного управления или органов управления, воинских частей и организаций, в том числе информацию о дислокации или передислокации органов военного управления или органов управления, объединений, соединений, воинских частей, организаций и подразделений, не отнесенную к перечню сведений, составляющих государственную тайну;

б) нарушение запрета иметь при себе при исполнении обязанностей военной службы электронные изделия бытового назначения, в которых могут храниться или которые позволяют с использованием сети «Интернет» распространять или предоставлять аудио-, фото-, видеоматериалы и данные геолокации, в следующих случаях: участие в боевых действиях, выполнение задач в условиях чрезвычайного или военного положения, вооруженных конфликтов, участие в деятельности по поддержанию или восстановлению международного мира и безопасности либо пресечению международной террористической деятельности за пределами территории Российской Федерации; несение боевого дежурства, боевой службы, службы в гарнизонном наряде, исполнение обязанностей в составе суточного наряда; участие в учениях или походах кораблей; нахождение на территории воинской части в течение

установленного распорядком дня служебного времени или в другое время, если это вызвано служебной необходимостью; прохождение военных сборов; оказание помощи органам внутренних дел, другим правоохранительным органам по защите прав и свобод человека и гражданина, охране правопорядка и обеспечению общественной безопасности; участие в предотвращении и ликвидации последствий стихийных бедствий, аварий и катастроф [2].

Кроме того, Указом Президента Российской Федерации от 06 мая 2020 г. № 308 [3] внесены соответствующие изменения в УГиКС ВС РФ, согласно которым начальнику караула (ст. 171), помощнику начальника караула (ст. 191), оператору технических средств охраны (ст. 195), разводящему (ст. 196) и часовому (ст. 209) во время несения службы, а также в караульном помещении (ст. 268) запрещено иметь при себе электронные изделия бытового назначения, в которых могут храниться или которые позволяют с использованием сети «Интернет» распространять или предоставлять аудио-, фото-, видеоматериалы и данные геолокации [2]. Изложенное выше свидетельствует о более высокой степени ответственности военнослужащих за использование в период выполнения своих функциональных обязанностей сети «Интернет» и соответствующих электронных устройств, обеспечивающих выход в сетевое пространство. Усиление запрета на аналогичную деятельность сотрудников органов внутренних дел не сопровождается адекватными мерами нормативно-правового реагирования, поскольку согласно существующей точки зрения, особенности служебной деятельности сотрудников органов внутренних дел не позволяют обеспечить радикализацию запрещающих и ограничительных мер в части онлайн-коммуникации в период выполнения ими своих служебных обязанностей.

Подводя итог, в заключение представляется необходимым заметить следующее: во-первых, существующая система запретов и ограничений сотрудниками органов внутренних дел и военнослужащими на использование возможностей сети «Интернет» и ряда электронных устройств является необходимым шагом и обоснована с точки зрения существующих вызовов и угроз современного информационного общества; во-вторых, сравнительный анализ нормативно закрепленных видов нарушений за нарушение порядка обращения к сети «Интернет» и использования сотрудниками органов внутренних дел и военнослужащими некоторых электронных устройств подтверждает необходимость внесения изменений в Дисциплинарный устав органов внутренних дел, по аналогии с ДУ ВС РФ.

1. Федеральный закон от 30 ноября 2011 г. № 342-ФЗ «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства РФ, 05 декабря 2011. - № 49 (ч. 1). - Ст. 7020.
2. Указ Президента РФ от 10 ноября 2007 г. № 1495 «Об утверждении общевоинских уставов Вооруженных Сил Российской Федерации» // Собрание законодательства РФ, 19 ноября 2007. - № 47 (ч. 1). - Ст. 5749.
3. Указ Президента РФ от 06 мая 2020 г. № 308 «О внесении изменений в некоторые акты Президента Российской Федерации» / Официальный интернет-портал правовой информации «<http://www.pravo.gov.ru>», 06 мая 2020 г. // СПС КонсультантПлюс
4. Методические рекомендации МВД России от 13 марта 2020 г. № 1/2704 «О правилах поведения и организационной защите персональных данных сотрудников органов внутренних дел и их близких в сети «Интернет». - 17 с. (документ официально опубликован не был)
5. Кондрашов А.Е. Соцсеть - находка для агентов // Аргументы недели. - 2020. - № 18 (712). - 13 мая.
6. Chesney R., Citron D.K. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security // California Law Review. - 2019. - P. 1753-1820.