УДК 343.9

Социальный контроль в VUCA-мире и «обществе наблюдения»: состояние, тренды и этические проблемы

Комлев Ю.Ю.
Доктор социологических наук,
профессор кафедры философии, политологии, социологии и психологии
Казанского юридического института МВД России

В статье описаны технологическая специфика «общества наблюдения», а также состояние, основные тренды и этические проблемы в сфере реализации цифрового социального контроля. Предложены меры совершенствования самоконтроля на пути формирования основ цифрового гражданства.

Ключевые слова: цифровизация, сетевизация, «общество наблюдения», VUCA-мир, киберпреступность, кибердевиантность, искусственный интеллект, «большие данные», цифровое гражданство, цифровая грамотность, цифровой этикет, самоконтроль

В преобладающих практиках социального контроля еще на рубеже XXI в. был обозначен сдвиг в сторону структурно-средового противодействия группам криминального риска. Т. Дамм назвал этот процесс переходом от «надзора» к «слежению», или мониторингу [1, p. 186]. Идею слежения зафиксировал и Жиль Делез, назвав мир постмодерна «обществом контроля», в котором речь больше идет не об «аресте и возвращении преступника к нормальной жизни» после совершения им преступления, а об осуществлении слежения за действиями индивидов, представляющих опасность, что позволяет принимать упреждающие меры [2].

Как известно, в промежутке между зарождением цивилизации и 2003 г. было произведено 5 эксабайт информации, столько же теперь создается каждые два дня и темпы все увеличиваются. Прошло совсем немного времени и благодаря интернету, тотальной цифровизации и сетевизации социума, стремительному развитию цифровой экономики, внедрению сквозных цифровых технологий, как тропический циклон, в нашу повседневность ворвался *VUCA*-мир со своей изменчивостью (*Volatility*), неопределенностью (*Uncertainty*), сложностью (*Complexity*) и неоднозначностью (*Ambiguity*).

Технологии *Big Data* и искусственного интеллекта, интернета вещей, виртуальной и дополненной реальностей, робототехники, беспроводной связи и биометрии (распознавание лиц, сканирования отпечатков пальцев), определения местоположения изменили качество, ценность и объемы информации, используемой человеком в XXI в. Космические скорости технологических и социальных изменений сводят на нет все долгосрочные и среднесрочные прогнозы, радикально меняют и усложняют жизнь современного человека, общества и государства.

В цифровой экономике, сфере принятия решений и других отраслях постоянно растает спрос на актуальные цифровые инструменты и сквозные технологии. Ежегодный рост рынка *Big Data* и облачных технологий в совокупности составляет 20,8 %, искусственного интеллекта (машинное обучение, нейронные сети, глубокое обучение) – 39,7 %, распределенного реестра (блокчейн) – 80,2 %. Цифровой мир, который характеризует акроним *VUCA*, не только ускоряет технологические процессы, повышает производительность труда, прибыль, минимизирует издержки, снижает ошибки, связанные с «человеческим фактором», но и создает проблемы.

Девиантологи, в частности, обращают внимание на технологические возможности для роста киберпреступности и других проявлений кибердевиантности, на проблемы и необходимость совершенствования социального контроля в этой сфере. Эксперты из МВД России свидетельствуют о том, что доля регистрируемых деликтов, совершаемых в интернете или в компьютерной сфере, постоян-

но растет и в настоящее время превышает 25 % от общего числа всех преступлений [3].

Киберпреступления и другие цифровые девиации все больше направлены не на компьютеры, а на пользователей интернета, социальных сетей, коммуникативных технологий и цифровых платежных систем. Если стабильно растет киберпреступность, то, следуя логике *social bonding theories*, что-то не так обстоит с социальным контролем, несмотря на его цифровизацию.

Повсеместно в общественных пространствах Европы, США, России и особенно Китая устанавливаются видеокамеры, связанные с алгоритмами распознавания и обработки больших данных. Китайские полицейские в смарт-шлемах уже несколько лет контролируют правопорядок на улицах, дополняя систему стационарного видеонаблюдения. Системы видеоконтроля широко используют технологию искусственного интеллекта, и сегодня многие аналитики не без оснований называют цифровое общество «обществом наблюдения».

Обзор ряда зарубежных и отечественных работ по организации цифрового социального контроля для противодействия киберпреступности и кибердевиантности позволяет обозначить ряд особенностей, тенденций и этических проблем в этой сфере [4-7]. Наиболее важные из них состоят в следующем:

1. Существенным трендом является рост использования «умных вещей», цифровых видеокамер и биометрических наблюдений в общественных местах, основанных на технологии распознавания лиц. Лидером по темпам установки систем видеонаблюдения является КНР. За последние два десятилетия в этой стране создана всеобъемлющая система видеонаблюдения. По некоторым данным еще в 2020 г. был пройден порог установки 600 млн видеокамер в общественных местах в рамках государственной системы социального кредита, суть которой в том, чтобы с помощью тотального цифрового социального контроля подвести каждого гражданина к «правильному» поведению.

2. Активно развиваются интеллектуальные системы фиксации и цифровой идентификации отпечатков пальцев, рисунков сетчатки и радужной оболочки, голосовых паттернов и других идентификаторов. Так, например, организован цифровой социальный контроль в индийской интегрированной интеллектуальной системе «Адхаар». Среди прочих возможностей она по аналогии с китайской системой социальных кредитов определяет доступ к основным государственным услугам, таким как: голосование, регистрация, уплата налогов, доступ к пенсиям, пособиям по безработице.

3. Под влиянием пандемии *COVID*-19 произошло дальнейшее расширение форм биометрического наблюдения с использованием тепловизоров и других девайсов. Ярким примером является быстрое внедрение мобильных приложений, используемых для отслеживания контактов, соблюдения карантина, мониторинга социального дистанцирования или отслеживания симптомов и состояния здоровья, других цифровых следов. Опыт обработки *QR*-кодов широко известен в России, где велись наблюдения с помощью сети из 100 тыс. видеокамер и искусственного интеллекта для распознавания и отслеживания лиц, помещенных в карантин.

4. Новым подходом к совершенствованию систем видеофиксации с целью надзора и мониторинга за девиантами стало использование в совокупности алгоритмических решений с помощью аналитики *Big Data* и искусственного интеллекта. Привлечение таких систем состоялось в правоохранительной и судебной деятельности, в управлении исправительными учреждениями. Так, например, происходит при вынесении альтернативных решений относительно заключенных в рамках системы *COMPAS* (США), созданной как инструмент алгоритмического подсчета баллов для определения необходимости прохождении испытательного срока, оценки риска совершения преступления, что обеспечивает принятие судебных ограничений. Накоплен опыт использования искусственного интеллекта (приложение *Prometea*, Аргентина) для быстрого принятия типовых судебных решений. Искусственный интеллект для углубленного анализа судебной и правоприменительной практики используется в странах Евросоюза. На еще большее разнообразие в применении искусственного интеллекта посягнули китайские суды, где цифровыми приложениями охвачены не только подача цифровых исков, но и проверки личности в системе социального кредита, а также продвижение мобильных электронных судебных процессов.

5. Наблюдение ведется и в социальных сетях за онлайн-активностью и персональными данными отдельных лиц, представителей «проблемных» групп, пропагандирующих экстремизм и террор, вовлечение в самоубийство. У технологических компаний, таких как *Google,* есть приложения, которые отслеживают не только девиантов, но и «шпионят» за другими пользователями интернета. Они, нарушая конфиденциальность, анализируют электронную почту, сообщения, календари и личные предпочтения, местоположение, просмотр веб-страниц и другие персональные данные пользователей. Так, к примеру, приложения *Angry Birds* и *Shazam*, автоматически ведут сбор данных о местоположении и адресе мобильного устройства. Многие из таких инструментов разработаны с минимальной защитой от злоупотреблений и, увы, не всегда отвечают стандартам кибербезопасности, что позволяет похищать и обмениваться данными с целью вымогательства, шантажа, кибербуллинга.

6. Для противодействия распространению кибердевиантности совершенствуется контроль и ре-

стрикции свободного доступа к информации в интернете. Путем целенаправленного его ограничения с помощью блокировки адреса интернет-протокола («*IP*»), системной («*DNS*») фильтрации. Этот опыт накоплен в Китае с использованием интернет-цензуры, известной как «Великий брандмауэр». США, Китай, Россия и другие страны оказывают все большее давление на технологические компании, чтобы те удаляли нежелательный контент. Китай и Россия, Бразилия, Турция для обеспечения своего «киберсуверенитета» принимают законы, направленные на создание национального, автономного интернета. Например, в России «интернет-трафик» в пределах страны может проходить только через пункты интернет-обмена (*IXP*), которые предварительно одобрены Роскомнадзором. В некоторых странах возможен и полный запрет доступа к нежелательным ресурсам или существенное замедление трафика. Китайский Закон о кибербезопасности 2017 г. расширил тенденцию к кибер-суверенитету страны. Среди всего прочего он требует, чтобы операторы сетевых услуг хранили личные данные внутри страны и предоставляли их властям по запросу, вводя оценки безопасности. Это вынуждает зарубежные технологические компании приспосабливаться к внутренним правилам Китая и других стран с рестриктивным законодательством по отношению к глобальной сети.

7. Аналитики усматривают в усилиях по обеспечению киберсуверинетета в Китае и других странах развитие «цифрового авторитаризма» для «контроля, подавления и манипуляций» в интересах государства. Впрочем, очевидно, что не меньшее количество фактов ограничений, а то и предвзятости, цензуры в киберпространстве видно на примере западных демократий. Достаточно вспомнить последнюю избирательную кампанию в США, где Д. Трамп стал жертвой многочисленных *fake-news* в социальных сетях и цифровых медиа, которые контролировали демократы. Пандемия поспособствовала распространению массовой слежки на основе технологий распознавания лиц и других биометрических данных. Такое видеонаблюдение ведется, как правило, без ведома и учета мнения общественности, для мониторинга социального дистанцирования и выявления нарушений директив по безопасности для здоровья.

8. Еще одной формой рестрикции информационного потока в интернете на таких платформах, как *Facebook, Twitter, Instagram,* становится автоматическая цензура. Она включает в себя сложные методы фильтрации контента, которые используют алгоритмы, основанные на машинном обучении (искусственный интеллект). Эти инструменты работают в реальном времени и явно не уведомляют пользователя, что делает их незаметными. Приватизированная цензура технологических компаний может также приводить к манипуляциям, распространять ложные новости, подавлять голоса несогласных в своих коммерческих и политических интересах. Здесь кроются реальные проблемы этического плана и наступления на права человека при реализации цифрового социального контроля.

9. Практики цифрового социального контроля над кибердевиантностью нередко выходят за девиантологические пределы и распространяются на гражданские и политические права (например, свободу выражения мнений, право на неприкосновенность частной жизни, свободу собраний и др.). Эксперты отмечают, что в «обществе наблюдения» цифровые инструменты «все чаще используются для подталкивания, смещения, направления, провоцирования, контроля, манипулирования и ограничения человеческого поведения». Кроме того, алгоритмические системы как основа для принятия решений непрозрачны, а возможности обжалования и получения возмещения в случаях злоупотреблений очень ограничены, если вообще существуют.

10. Девиантологи и юристы справедливо отмечают отставание в развитии формального социального контроля в цифровой сфере. Это относится и к совершенствованию международного законодательства, которое на данный момент сводится к Будапештской конвенции Совета Европы о компьютерных преступлениях (2001 г.) и национальному законодательству. Высказываются существенные претензии к законодателям относительно определения составов киберпреступлений (гл. 28 УК РФ, ст.ст. 272-274) и структур, занятых противодействием киберпреступности. Как известно, не завершен процесс создания киберполиции в РФ, декларация о формировании которой была заявлена официально еще в конце 2020 г.

11. Отечественные исследователи обращают внимание на необходимость повышать техническую грамотность населения, чтобы снизить кибервиктимизацию, развивать «массовую и индивидуальную культуру безопасности при использовании цифровых технологий». Со своей стороны, полагаю, что вопросы самоконтроля не менее важны, чем совершенствование системы формального социального контроля: его правовых и цифровых вариантов.

Вполне уместно ставить вопрос о комплексной, начиная с детства, системе подготовки «цифровых граждан» – людей *VUCA*-мира, подготовленных к использованию возможностей цифровых технологий и защите от их опасных последствий, в том числе в киберпространстве. Такой подход удачно структурировал М. Риббл, который выделил девять основных элементов цифрового гражданства. Они включают в себя цифровой доступ, цифровую торговлю, цифровую коммуникацию, цифровую грамотность, цифровой этикет, цифровое законодательство, цифровые права и обязанности, цифро-

вое здоровье и благополучие, цифровую безопасность [8].

В обеспечении самоконтроля чрезвычайно *важны цифровая грамотность, цифровой этикет, цифровые права и обязанности, цифровая безопасность и конфиденциальность.* Цифровая грамотность как результат постоянного обучения, социализации, начинается с детского сада. Технологии быстро меняются, и на рынке цифровых услуг появляются новые устройства, сервисы, информационные ресурсы, которые легко усваиваются детьми. Цифровой этикет – это нормы правильного поведения в интернете и социальных сетях, усвоенные в ходе социализации, которыми следует руководствоваться при использовании различных, в том числе банковских сервисов и цифровых услуг. Цифровые права и обязанности – атрибут тех людей, кто становится участником цифровых коммуникаций. Эта область цифрового гражданства предоставляет право с учетом ограничений по возрасту на доступ в интернет и к иным информационным ресурсам. Цифровая безопасность и конфиденциальность состоят в защите личных данных пользователя с помощью надежных паролей, антивирусных программ, резервного копирования данных. Таким образом, элементы цифрового гражданства, усвоенные в ходе социализации, могут быть основой для эффективного самоконтроля и существенного снижения рисков цифровой виктимизации в наступившем *VUCA*-мире.

Литература:

1. Dumm T. The New Enclosures: Racism in the Normalized Community // Reading Rodney King, Reading Urban Uprisings / Ed. R. Gooding-Williams. – New York: Routledge, 1993. – 276 p.
2. Deleuze G. Postscript on Control Societies // Negotiations, 1972–1995. -New York: Columbia University Press, 1995. – P. 177-182.
3. Соловьева О. Доля цифрового криминала в России превысила 25 %. – URL: https://www.ng.ru/economics/2021-08-03/1_8215_economics2.html (дата обращения: 19.05.2022).
4. Овчинский В.С. Контроль над преступностью в цифровом обществе. – URL: https://zavtra.ru/blogs/kontrol_nad_prestupnost_yu_v_tcifrovom_obshestve (дата обращения: 19.05.2022).
5. Khalil L. Digital Authoritarianism, China and COVID – Lowy Institute. – URL: https://www.lowyinstitute.org/publications/digital-authoritarianism-china-and-covid (дата обращения: 19.05.2022).
6. Digital technologies as a means of repression and social control. – URL: https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2021)653636(дата обращения: 19.05.2022).
7. Шипунова Т.В. Преступность в цифровом обществе: причины и возможности противодействия // Социальная безопасность в евразийском пространстве: материалы Международной научной конференции (14 декабря 2021 г.) / Под. ред. И.А. Грошевой. – Тюмень: Филиал АНО ВО «ИДК» в Тюменской области, 2022. – С. 473-480.
8. Ribble M. Digital citizenship: using technology appropriately. – URL: http://www.digitalcitizenship.net/Nine_Elements.html (дата обращения: 19.05.2022).

Social Control in the VUCA-World and the "Observation Society": Status, Trends and Ethical Issues

Komlev Yu.Yu.
Kazan Law Institute of the Ministry of Internal Affairs of Russia

The article describes the technological specifics of the "observation society", as well as the state, main trends and ethical problems in the implementation of digital social control. Measures to improve self-control on the way to the formation of the foundations of digital citizenship are proposed.

Key words: digitalization, networkization, "observation society", VUCA-world, cybercrime, cyberdeviance, artificial intelligence, "big data", digital citizenship, digital literacy, digital etiquette, self-control