УДК 34

Актуальные проблемы развития цифрового права в контексте безопасности личности

Лукошкин Анатолий Анатольевич

Аспирант,
Московская Финансово-Юридическая Академия,
117342, Российская Федерация, Москва, ул. Введенского, 1а;
e-mail: yalukosh@yandex.ru

Аннотация

Безопасность личности выполняет особую роль в публично-правовых отношениях современного мира. Вопросы реализации финансовых и налоговых правоотношений активно развиваются параллельно динамике цифрового развития и создают дополнительные риски и угрозы человека в цифровом пространстве. Цифротизация активно реализуется в программах судебного правоприменения в отраслях частного права и его автоматизирования. Примечателен опыт КНР в принципах справедливого и публичного права путем цифровитизации всех судебных процессов в режиме «онлайн» выполненной программой развития «Верховного народного суда Китая. В России вопросы цифровой безопасности регулируются законодательством, в том числе Федеральным законом "О безопасности информации". Этот закон устанавливает требования к защите информации, которые должны соблюдаться операторами информационных систем. Кроме того, в России действует специализированный орган по защите информации - Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). В Китае также существует законодательство, регулирующее цифровую безопасность, включая Закон о безопасности сети информации. Этот закон устанавливает требования к защите информации сети и обязанности сетевых операторов по обеспечению безопасности информации. Кроме того, Китай имеет известную "Великую китайскую стену" - систему технических средств централизованного контроля и фильтрации интернет-трафика.

Для цитирования в научных исследованиях

Лукошкин А.А. Актуальные проблемы развития цифрового права в контексте безопасности личности // Вопросы российского и международного права. 2024. Том 14. № 9А. С. 71-78.

Ключевые слова

Цифровитизация, цифровое право, безопасность личности, цифровые угрозы, киберугрозы, кибермошенничество.

Введение

Публично-правовой механизм обеспечения безопасности личности в цифровой среде обладает высокой актуальностью в рамках роста влияния цифровой среды на развитие правовых отношений между субъектами права. Планомерно объекты права в силу роста цифровитизации занимают все большую роль в цифровом пространстве, например, денежные отношения и цифровые валюты, система голосования и цифровые контракты на децентрализованных системах. Более того стоит отметить расширение параметров определения как такого субъекта права в качестве Искусственного интеллекта.

С точки зрения публично-правовых механизмов стоит рассмотреть активное развитие в рамках правовых процессов. Судебные процессы представляют сложную процедуру разрешения конфликтов, в многом как правило требующее справедливой оценки и вердикта. Преобладающие принципы это: осуществление правосудия только судом; независимость, неприкосновенность, несменяемость судей; открытое разбирательство дел в суде; состязательность и равноправие сторон; сочетание коллегиального и единоличного порядка рассмотрения дел. С точки зрения искусственного интеллекта возможно спрогнозировать вероятность повторного правонарушения, определить комплекс эффективных решений на основании статистических и математических решений, но крайне сложно учесть специфику каждого судебного процесса и все условия, принимаемые судом, человеком соответственно для вынесения приговора.

Машинное обучение в свою очередь позволяет создать более твердую прецедентную модель, как прикладной инструмент в разрешении правовых споров. Более того данный инструмент снижает риск ошибки в судебной практике и юридической деятельности. [Иванова, www..., с. 3-4]

Безопасность личности в понимании цифрового права является ключевым параметром обеспечения прозрачности правового регулирования и комплексных законодательных актов создающих данную безопасность. Примером для рассмотрения данного вопросы выступает активная автоматизация судебной системы, например, в КНР. Искусственный интеллект будет поддерживать суды КНР с 2025 года при этом заменить живых судей ИИ не сможет, по позволит упростить и облегчить рутинную работу и типовые процессы. Актуальными мерами автоматизации принято относить автоматизацию процессов домашнего быта, производства товаров, обслуживания, предоставления коммерческих услуг.

Основное содержание

Наступает период глубокого освоения юридических аспектов различными результатами программного обеспечения. Верховный народный суд (SPC) - это Верховный суд Китая, по состоянию на июнь 2017 года в составе SPC 367 судей. Основными сферами компетенции SPC являются рассмотрение дел и вынесение судебных толкований. «SPC» активно использует цифровой прогресс.

Основные программы судебного автоматизирования «SPC»:

– Система автоматизации делопроизводства. Система может помочь судьям в рассмотрении дел, таких как: передача судебных решений по одному и тому же типу дел судьям для справки (т. Е. Механизм «продвижения схожих дел»); автоматическое составление

приговора и автоматическое исправление ошибок в приговоре. Китайские суды хотят включить в систему искусственный интеллект, чтобы помогать судьям принимать решения, повышать их эффективность или предупреждать судей о ненормальных решениях, чтобы контролировать их поведение. [Механизм работы китайского электронного правосудия, www...]

– Система управления судебными процессами. Поскольку информация о каждом судье и каждом деле регистрируется в системе автоматизации делопроизводства, и система была подключена ко всем судам в стране, SPC может знать все суды, всех судей и все дела в стране в режиме реального времени. Кроме того, руководство суда может в режиме реального времени получать информацию о каждом судье и каждом деле. Это еще больше укрепило управленческий потенциал китайских судов. Другими словами, иерархическая структура китайских судов была дополнительно усилена.
– Информация о судебном процессе и о его решениях в Китае. SPC создал «Китайскую судебную информацию онлайн» и требует, чтобы все суды по всей стране предоставляли сторонам и их адвокатам информация о судебном процессе их дела, включая: информацию о каждом узле судебного разбирательства, стенограммы, аудио и видео судебного заседания, файлы дела и все юридические документы, которые должны быть вручены сторонам.

Российская судебная система развивается не менее эффективно. В Арбитражном суде Московского округа с 2006 года внедрен программный комплекс «Судебно-арбитражное делопроизводство» (далее - ПК САД). ПК САД предназначен для автоматизации процессов судебного делопроизводства. [Государственная автоматизированная система Российской Федерации «Правосудие», www...]

Развитие цифрового общества находится на самой активной точке своего роста, юридические аспекты актуальны как никогда. Для легализации цифровых активов в правовом поле 1 января 2021 года в России вступил в силу Закон о цифровых финансовых активах и цифровой валюте. В повестке цифрового рубля и цифровитизации общества данный закон играют значительную роль в построении цифровой экономики и правовой дисциплины. Голосование на выборах президента в этом году в г. Москве были проведены с возможностью использования цифровой подписи на децентрализованной платформе онлайн. При этом количество электронного документооборота и правовых действий путем цифровых решений неуклонно растет.

Государственная автоматизированная система РФ «Правосудие» - это территориально распределенная автоматизированная информационная система, предназначенная для формирования единого информационного пространства судов общей юрисдикции и системы Судебного департамента при Верховном Суде Российской Федерации (СД), обеспечивающая информационную и технологическую поддержку судопроизводства на принципах поддержания требуемого баланса между потребностью граждан, общества и государства в свободном обмене информацией и необходимыми ограничениями на распространение информацииБудущее развитие ГАС «Правосудие» должно обеспечить повышение эффективности деятельности всей судебной системы РФ, включая объекты районного уровня и мировую юстицию.

С точки зрения обширного круга цифрового пространства в судебной деятельности проблематика защиты и обеспечения прав граждан по-прежнему является острой. Количество киберугроз представлено возрастающим трендом.

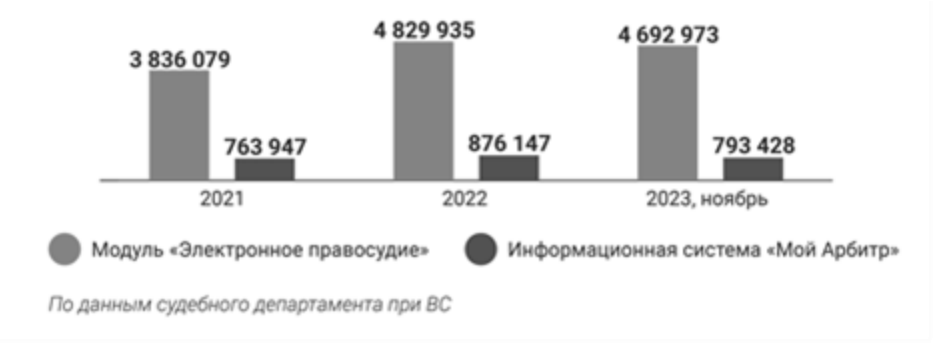

Рисунок 1 - Количество документов, поданных в суды в электронном виде [Государственная автоматизированная система Российской Федерации «Правосудие», www...]

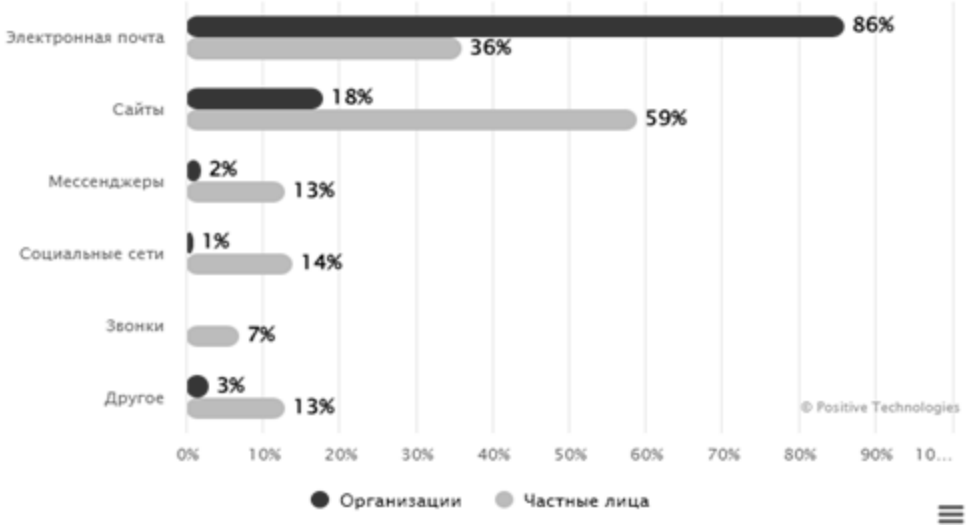

Рисунок 2 - Динамика мошенечества по категориям 2023 год. [Угрозы кибербезопасности, www...]

Социальная инженерия остается одним из наиболее популярных методов атак на организации (50%) и частных лиц (91%). Основным каналом социальной инженерии в атаках на организации является электронная почта (86%), а на частных лиц — веб-ресурсы и сервисы (59%).

Отличительной чертой I квартала стала повышенная активность правоохранительных органов и спецслужб в отношении представителей киберпреступного мира. Если ранее деятельность злоумышленников пытались пресечь или осложнить преимущественно в правовом поле, то сейчас правоохранители переходят к активным действиям.

В рамках правового поля нарушителя относящиеся к категориям хакерам-шантажистам, пойманные следствием, подлежат ответственности не только за незаконный доступ к компьютерной информации (272 УК РФ), но и по статье о вымогательство (163 УК РФ).

Цифровые проблемы безопасности в современном обществе становится предметов цивилизованного характера и залогом благополучия. Цель правовой деятельности в обеспечении безопасности личности его прав и свобод. Скорость и гибкость технологий позволяет не только улучшать благополучие общества, но и играет на руку преступным

действиям, позволяя расширять спектр технологий в совершении противоправных действий в отношении других граждан.

Рисунок 3 - Динамика результатов кибератак по категорям 2023 г. [Угрозы кибербезопасности, www...]

С точки зрения современных бытовых вопросов в которых денежные средства и основная информация о человеке находится в рамках цифровых носителей информации, важно понимать, что данные устройства и являются целью мошенников. Проблематика состоит в том, что информации в данных устройствах может выступать одновременно источником для обеспечения безопасности одного и нарушением безопасности другого гражданина.

В условиях обвинения цифровые устройства как правило содержат необходимую доказательную базу, но обвиняемый не обязан предоставлять доступ к своим устройствам. При этом учитывая практику Верховного суда Российской Федерации, в котором решения относительно обвиняемых принимаются по следящему принципу: «Отказ обвиняемого от показаний не может быть истолкован против него либо являться даже косвенным подтверждением виновности». Соответственно отказ от предоставления данных на цифровых устройствах, которые играют прямую роль в построении справедливого вердикта большинства судебных дел в современном обществе. Согласно презумпции невиновности, фигурант не обязан доказывать свою невиновность, а бремя доказывания обвинения и опровержения доводов, приводимых в защиту, лежит на стороне обвинения, напоминает высшая инстанция. [Возженков, 2023, с. 140-143]

Конституционно-правовое регулирование обеспечения прав и свобод человека в РФ может улучшено путем расширения процессов автоматизации. По мнению председателя ВС РФ, Вячеслава Лебедева «Гуманизм — важный принцип Уголовного кодекса, который обеспечивает безопасность человека». суды сами учитывали и способствовали соблюдению такого принципа. Поэтому гуманизация законодательства будет системно продолжена». Именно данный принцип является самым сложным для применения в структуре цифрового права.

Заключение

Для решения проблемы законодательной эффективности необходимо расширения инструментов технической базы обеспечения соблюдения нормативно-правовых актов. В свою очередь регистраторы доменных имен в свою очередь требуют предоставления полной информации о владельце, о целях, характере размещаемой информации. Активную роль в формировании благонадежных источников выполняют органы государственной политики и контроля. Роскомнадзор основанный в 2008 году ведет активную борьбу с сервисами, несущими потенциальный риск для граждан. Характер публикуемой информации пользователями различных социальных сетей, субъектов интернет-пространства. [Карпов, 2021, с.88-94]

Правоприменительная практика требует развития цифровых угроз и в международном праве. При регулярно увеличивающемся количестве кибератак и киберугроз в 2011 году, Россия, КНР, Узбекистан и Таджикистан вынесли на обсуждение 66-ой сессии ООН меморандум «"Международные критерии поведения для информационной безопасности"». Стоит отметить документ является первым сравнительно всеобъемлющим и систематичным документом относительно международных правил об информационной и сетевой безопасности. [Терехов, 2021, с.230-232]

Важно понимать, что безопасность международного характера между государствами это прежде всего безопасность граждан внутри стран. Любые политические, экономические, военные и прочие конфликты оказывают серьёзное давление на граждан той или иной стороны.

Особую роль безопасности личности в правовой системе отношений играет не только эффективность правовой среды и её технической оснащенности, но и уровень осведомленности личности о её угрозах в этом пространстве.

Библиография

1. Возженков А.В. Обеспечение безопасности личности (политико-правовой аспект): монография. М.: РАГС, 2023. 182 с.
2. Карпов В.И. Теоретические основы обеспечения безопасности личности, общества и государства: учеб. пособие 2-е изд., доп. и перераб. М.: Юр. ин-т МИИТа, 2021. 236 с.
3. Лисина О. В. Конституционное ограничение прав и свобод человека и гражданина: понятие и пределы // Вестник ПАГС. – 2023. – №3. – 140 с.
4. Морозов И. Л. Государственная политика в сфере информационной безопасности по легитимации политического порядка современной России – тенденции, проблемы, решения // Общество: политика, экономика, право. –2023. – №9 (86). – Режим доступа:URL:https://cyberleninka.ru/article/n/gosudarstvennaya-politika-v-sfere-informatsionnoy-bezopasnosti-po-legitimatsii-politicheskogo-poryadka
5. Сапожников А.И. Административно-правовой режим общественной безопасности: дис.канд. юрид. наук. М., 2022. 198 с.
6. Терехов М.Г. Цифровое право. ЭКОНОМИКА. ПРАВО. ОБЩЕСТВО. 2021;(3):67-70. https://doi.org/10.21686/2411-118X-2021-3-70 с.
7. Государственная автоматизированная система Российской Федерации «Правосудие», сайт: некоммерч. интернет-версия. – URL: https://techportal.sudrf.ru/?id=234 (дата обращения: 20.02.2021).
8. Практика Верховного суда РФ по киберпреступлениям, сайт: некоммерч. интернет-версия. – URL: https://alrf.ru/news/praktika-verkhovnogo-suda-rf-po-kiberprestupleniyam/ (дата обращения: 25.01.2024).
9. Иванова А.П. Искусственный интеллект в области права: сайт: некоммерч. интернет-версия. – URL: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-v-sfere-prava-i-yuridicheskoy-praktike-osnovnye-problemy-i-perspektivy-razvitiya/viewer (дата обращения: 28.03.2024).
10. Механизм работы китайского электронного правосудия: сайт: некоммерч. интернет-версия. – URL: https://ru.chinajusticeobserver.com/a/how-chinese-e-justice-works (дата обращения: 15.02.2024).
11. Угрозы кибербезопасности: четвертый квартал 2023 г. сайт: некоммерч. интернет-версия. – URL: https://www.ptsecurity.com/ww-en/analytics/ (дата обращения: 21.02.2024).

Current problems of the development of digital law in the context of personal security

Anatolii A. Lukoshkin

Postgraduate student,
Moscow Academy of Finance and Law,
117342, 1a, Vvedenskogo str., Moscow, Russian Federation;
e-mail: yalukosh@yandex.ru

Abstract

Personal security plays a special role in the public relations of the modern world. The issues of the implementation of financial and tax legal relations are actively developing in parallel with the dynamics of digital development and create additional risks and threats to humans in the digital space. Digitalization is actively implemented in judicial enforcement programs in the fields of private law and its automation. The PRC's experience in the principles of fair and public law is noteworthy by digitalizing all trials online through the development program of the Supreme People's Court of China. In Russia, digital security issues are regulated by legislation, including the Federal Law on Information Security. This law establishes information protection requirements that must be respected by information system operators. In addition, Russia has a specialized information protection body - the Federal Service for Supervision of Communications, Information Technology and Mass Communications (Roskomnadzor). China also has legislation governing digital security, including the Information Network Security Act. This law establishes the requirements for the protection of network information and the responsibilities of network operators to ensure the security of information. In addition, China has the famous "Great Wall of China" - a system of technical means for centralized control and filtering of Internet traffic. Both countries are also actively developing their cyber weapons and cyber capabilities to protect their information infrastructure from cyber attacks. Recently, it was announced the creation of a "digital iron curtain" in Russia, which will ensure the security of the country's critical information infrastructure.

For citation

Lukoshkin A.A. (2024) Aktual'nye problemy razvitiya tsifrovogo prava v kontekste bezopasnosti lichnosti [Current problems of the development of digital law in the context of personal security]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 14 (9A), pp. 71-78.

Keywords

Digitalization, digital law, personal security, digital threats, cyber threats, cyber fraud.

References

1. Vozhenkov A.V. Ensuring personal security (political and legal aspect): monograph. M.: RAGS, 2023. 182 p.
2. Karpov V.I. Theoretical foundations of ensuring the security of the individual, society and the state: studies. the manual 2nd ed., additional and revised. M.: Law Institute of MIITa, 2021. 236 p.
3. Lisina O. V. Constitutional restriction of human and civil rights and freedoms: concept and limits // PAGS Bulletin. – 2023. – №3. – 140 S.

4. Morozov I. L. State policy in the field of information security to legitimize the political order of modern Russia – trends, problems, solutions // Society: politics, economics, law. -2023. – №9 (86). – Mode доступа: URL: https:// cyberleninka.ru/article/n/gosudarstvennaya-politika-v-sfere-informatsionnoy-bezopasnosti-po-legitimatsii-politicheskogo-poryadka
5. Sapozhnikov A.I. Administrative and legal regime of public safety: dissertation of the candidate. Jurid. M., 2022. 198 p.
6. Terekhov M.G. Digital law. Economy. right. SOCIETY. 2021;(3):67-70. https://doi.org/10.21686/2411-118X-2021-3-70 S.
7. The State automated system of the Russian Federation "Justice", website: non-commercial. the online version. – URL: https://techportal.sudrf.ru/?id=234 (date of appeal: 02/20/2021).
8. The practice of the Supreme Court of the Russian Federation on cybercrimes, website: non-commercial. the online version. – URL: https://alrf.ru/news/praktika-verkhovnogo-suda-rf-po-kiberprestupleniyam / (date of access: 01/25/2024).
9. Ivanova A.P. Artificial intelligence in the field of law: website: non-commercial. the online version. – URL: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-v-sfere-prava-i-yuridicheskoy-praktike-osnovnye-problemy-i-perspektivy-razvitiya/viewer (date of access: 03/28/2024).
10. The mechanism of Chinese electronic justice: website: non-commercial. the online version. – URL: https://ru.chinajusticeobserver.com/a/how-chinese-e-justice-works (date of application: 02/15/2024).
11. Cybersecurity threats: the fourth quarter of 2023. website: non-commercial. the online version. – URL: https://www.ptsecurity.com/ww-en/analytics / (date of access: 02/21/2024).