Четырнадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию

Distr.: General
23 January 2020
Russian
Original: English

Киото, Япония, 20–27 апреля 2020 года

Пункт 6 предварительной повестки дня*
Международное сотрудничество и техническая помощь в предупреждении всех форм преступности и борьбе с ними

Семинар-практикум 4. Современные тенденции в области преступности, последние изменения и новые решения, в частности использование современных технологий как средства совершения преступлений и инструмента борьбы с преступностью**

Справочный документ, подготовленный Секретариатом

Резюме

В настоящем справочном документе рассматривается влияние технологий, которые являются палкой о двух концах: они не только дают возможность совершать преступления, но и способствуют их предупреждению, выявлению и пресечению. С учетом этого обстоятельства в данном документе принят двухуровневый подход к объяснению зарождающегося фундаментального дуализма: роли технологий в поиске решений по охране правопорядка, судебному преследованию и обеспечению успешной работы системы уголовного правосудия, с одной стороны, и более мрачной роли технологий в совершенствовании методов деятельности преступников и организованных преступных групп — с другой. В ходе анализа учитываются изменения в конкретных областях и рассматриваются два сквозных аспекта: важность подготовки кадров, междисциплинарных подходов и синергического взаимодействия соответствующих заинтересованных сторон для получения представления о нынешних преимуществах технологий и их потенциале в деле устранения будущих угроз, связанных с совершением преступлений, и необходимость уделять должное внимание этическим вопросам и гарантиям соблюдения прав человека при использовании технологий для борьбы с преступностью.

* A/CONF.234/1.

** Секретариат хотел бы выразить признательность институтам сети программы Организации Объединенных Наций в области предупреждения преступности и уголовного правосудия, особенно Корейскому институту криминологии и Национальному институту юстиции Министерства юстиции Соединенных Штатов Америки, за помощь в подготовке и организации семинара-практикума.

I. Введение

1. В 1997 году, когда Программа Организации Объединенных Наций по международному контролю над наркотиками и Центр по международному предупреждению преступности были объединены в Управление по контролю над наркотиками и предупреждению преступности, переименованное в 2002 году в Управление Организации Объединенных Наций по наркотикам и преступности (УНП ООН), модернизированный вариант компьютера для игры в шахматы под названием “Deep Blue” стал первой компьютерной системой, победившей действующего чемпиона мира в матче шахматного турнира со стандартным контролем времени. В то время, несмотря на неуклонное развитие технологий, преступность оставалась относительно «низкотехнологичной», а интернет только начинал оказывать влияние на общество как определяющая технология «информационной эпохи».

2. Чуть больше чем за два десятилетия стремительное развитие интернета и информационно-коммуникационных технологий обеспечило условия для экономического роста и широкого доступа к жизненно важным услугам, создав наряду с этим новые возможности для преступной деятельности. Преступники неожиданно стали бенефициарами новых технологий и глобализации, поскольку эти достижения позволили им совершать преступления и извлекать из них выгоду за счет транснациональных операций и расширять свою незаконную деятельность и бизнес на цифровых платформах таким образом, чтобы снизить риски, в частности риск обнаружения[1].

3. С другой стороны, возникающие и существующие технологии открывают новые возможности для правоохранительной деятельности, расследования уголовных дел и судебного преследования. Повышение общественной безопасности и расширение возможностей правоохранительных органов и органов уголовного правосудия в области предупреждения преступности и борьбы с ней на основе технического прогресса могут оказать позитивное воздействие на достижение целей Повестки дня в области устойчивого развития на период до 2030 года, в частности цели 16 в области устойчивого развития.

4. В своем докладе «Эпоха цифровой взаимозависимости» Группа высокого уровня по цифровому сотрудничеству, учрежденная Генеральным секретарем в 2018 году в целях укрепления международного и многостороннего сотрудничества и внесения вклада в общественную дискуссию по вопросу о безопасном и инклюзивном цифровом будущем для всех, также обратила внимание на «два лица Януса». Как было отмечено, цифровые технологии доказали свою способность обеспечивать связь между людьми, разделенными культурными и географическими барьерами, углубляя взаимопонимание и обладая потенциалом, позволяющим обществам стать более мирными и сплоченными. Вместе с тем имеются примеры использования цифровых технологий для нарушения прав, подрыва принципа неприкосновенности частной жизни, поляризации общества и подстрекательства к насилию[2].

5. Настоящий справочный документ опирается на тематические рамки семинара-практикума 4 и расширяет их, как это отражено в руководстве для дискуссий на четырнадцатом Конгрессе[3]. Этот справочный документ состоит из отдельных разделов, каждый из которых отражает различные аспекты одной и той же основной проблемы, связанной с пребыванием правоохранительных органов и органов уголовного правосудия на распутье по причине стремительного возникновения новых технологий, которые могут не только способствовать эффективной работе полиции и играть важную роль в устранении традиционных

[1] Yury Fedotov, “In just two decades, technology has become a cornerstone of criminality”, *Huffington Post UK*, 23 October 2017.

[2] См. United Nations, “The age of digital interdependence”, June 2019, p. 17.

[3] A/CONF.234/PM.1, пункты 161–189.

недостатков в действиях по обеспечению полного соблюдения принципа верховенства права, но и часто использоваться преступниками в различных областях[4].

II. Технологии как средство совершения преступлений и инструмент борьбы с преступностью

A. Криптовалюты и виртуальные активы

6. В последние годы появились криптовалюты и виртуальные активы, которые привлекли инвестиции в платежную инфраструктуру, построенную с использованием их программных протоколов[5]. Пользователи криптовалют могут считать их применение целесообразным по целому ряду причин и владеть такими активами, выступающими в качестве спекулятивных инвестиций. Некоторые пользователи стремятся обеспечить конфиденциальность, связанную с более высоким уровнем анонимности сделок, в то время как другие просто хотят избежать надзора и/или контроля со стороны государства или банков в отношении их сделок, заключаемых на законных основаниях[6]. Сторонники криптовалют указывают на то, что комиссионные по сделкам ниже сборов традиционных банков в национальных валютах, хотя любые потери на обменном курсе и сборы, связанные с поставщиками услуг криптовалюты, могут снизить экономию затрат[7]. В местах, где традиционные банки недоступны, криптовалюты могут обеспечить функциональные возможности, связанные с традиционными платежными услугами[8]. Наконец, поскольку криптовалюта, как правило, не является государственной валютой, она может облегчить проведение трансграничных операций[9].

7. Несмотря на вышеизложенное, многие страны, разрешающие функционирование криптовалютных рынков, приняли законы по предотвращению отмывания денег, организованной преступности и финансирования терроризма[10], хотя на сегодняшний день, как представляется, террористы не используют криптовалюты в широких масштабах[11]. Указанная тенденция в области регулирования возникла в ответ на частое использование криптовалют для совершения незаконных покупок и покупок на черном рынке через интернет[12] и для внесения оплаты в случаях отмывания денег, применения схем Понци (финансовых

---

[4] Использование интернета и цифровых технологий в террористических целях, а также вопросы, связанные с киберпреступностью, рассматриваются в рабочем документе, подготовленном Секретариатом по пункту 6 повестки дня (A/CONF.234/7).

[5] Sesha Kethineni and Yin Cao, “The rise in popularity of cryptocurrency and associated criminal activity”, *International Criminal Justice Review*, 6 February 2019; Stearns Broadhead, “The contemporary cybercrime ecosystem: a multi-disciplinary overview of the state of affairs and developments”, *Computer Law and Security Review*, vol. 34, No. 6 (December 2018), pp. 1180–1196.

[6] Geoff Goodell and Tomaso Aste, “Can cryptocurrencies preserve privacy and comply with regulations?”, *Frontiers in Blockchain*, vol. 2, art. 4 (May 2019), pp. 1–20.

[7] Angela S. M. Irwin and Adam B. Turner, “Illicit Bitcoin transactions: challenges in getting to the who, what, when and where”, *Journal of Money Laundering Control*, vol. 21, No. 3 (July 2018), pp. 297–313.

[8] Ibid.

[9] Perri Reynolds and Angela S. M. Irwin, “Tracking digital footprints: anonymity within the bitcoin system”, *Journal of Money Laundering Control*, vol. 20, No. 2 (May 2017), pp. 172–189.

[10] United States, Law Library of Congress, Global Legal Research Center, *Regulation of Cryptocurrency around the World* (Washington D. C., 2018), June 2018.

[11] Cynthia Dion-Schwarz, David Manheim and Patrick B. Johnson, *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats* (Santa Monica, California, RAND Corporation, 2019).

[12] Reynolds and Irwin, “Tracking digital footprints”; Monica J. Barratt, Jason A. Ferris and Adam R. Winstock, “Safer scoring? Cryptomarkets, social supply and drug market violence”, *International Journal of Drug Policy*, vol. 35 (September 2016), pp. 24–31.

пирамид), вымогательства, шантажа (угрозы распределенных атак типа «отказ в обслуживании» (DDOS)) и мошенничества.

8. Концепции, применяемые к отмыванию денег с использованием наличных средств, также могут применяться к отмыванию денег с использованием криптовалют[13]. Процедура отмывания денег с помощью криптовалюты аналогична процедуре традиционного отмывания денег, но предусматривает использование технологий для достижения этой цели[14]. Кроме того, криптовалюты могут использоваться для облегчения ухода от налогов[15].

9. Растущую обеспокоенность также вызывает хищение криптовалюты[16]. Пользователи криптовалюты могут становиться жертвами мошенничества, направленного на ее кражу[17]. Кроме того, при совершении атак на физических лиц, компании или правительства в целях получения выкупа вымогатели часто выдвигают требования об оплате в криптовалюте.

10. Совершение преступлений, связанных с криптовалютами, облегчается в условиях, когда нормативные положения не позволяют идентифицировать пользователя или применить санкции, и при наличии возможностей для использования лазеек в нормативной базе. Различия между странами в нормативных положениях, касающихся криптовалют, позволяют пользователям осуществлять в одной стране деятельность, которая в других странах является незаконной[18].

11. Необходимо рассмотреть и осуществить ряд мер по предотвращению использования криптовалют в преступных целях. Подходы, предполагающие деанонимизацию сделок, могут способствовать выполнению сдерживающих и следственных функций. К данной категории могут относиться нормативные положения, требующие предоставления идентифицирующей информации (правила «знай своего клиента»)[19] или анализа операций с использованием машинного обучения или других методов наблюдения для выявления незаконных сделок[20].

12. Ограниченность знаний и навыков, необходимых для выявления или эффективного расследования криптовалютных схем, создает почву для расширения возможностей использования криптовалют в целях совершения незаконных действий[21]. Предупреждению и выявлению таких действий способствуют усилия, аналогичные усилиям Организации Объединенных Наций,

---

[13] Chad Albrecht and others, “The use of cryptocurrencies in the money laundering process”, *Journal of Money Laundering Control*, vol. 22, No. 2 (May 2019), pp. 210–216; Rolf van Wegberg, Jan-Jaap Oerlemans and Oskar van Deventer, “Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin”, *Journal of Financial Crime*, vol. 25, No. 2 (June 2018), pp. 419–435.

[14] Denis B. Desmond, David Lacey and Paul Salmon, “Evaluating cryptocurrency laundering as a complex socio-technical system: a systematic literature review”, *Journal of Money Laundering Control*, vol. 22, No. 3 (July 2019), pp. 480–497.

[15] Albrecht and others, “The use of cryptocurrencies in the money laundering process”; Saman Jafari and others, “Cryptocurrency: a challenge to legal system”, 10 May 2018.

[16] Garrick Hileman and Michel Rauchs, *Global Cryptocurrency Benchmarking Study* (Cambridge, United Kingdom of Great Britain and Northern Ireland, Cambridge Centre for Alternative Finance, 2017).

[17] Desmond and others, “Evaluating cryptocurrency laundering as a complex socio-technical system”.

[18] Angela S. M. Irwin and Caitlin Dawson, “Following the cyber money trail: global challenges when investigating ransomware attacks and how regulation can help”, *Journal of Money Laundering Control*, vol. 22, No. 1 (January 2019), pp. 110–131.

[19] Группа разработки финансовых мер, *Международные стандарты по противодействию отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения: рекомендации ФАТФ* (Париж, 2012 год).

[20] Irwin and Turner, “Illicit Bitcoin transactions”; Goodell and Aste, “Can cryptocurrencies preserve privacy and comply with regulations?”.

[21] Sesha Kethineni, Yin Cao and Cassandra Dodge, “Use of Bitcoin in darknet markets: examining facilitative factors on Bitcoin-related crimes”, *American Journal of Criminal Justice*, vol. 43, No. 2 (June 2018), pp. 141–157.

предпринимаемым в целях подготовки следователей по вопросам совершения преступлений, связанных с криптовалютой[22].

13. Эмитенты криптовалюты, регулирующие структуры и правоохранительные органы являются основными участниками мероприятий по предотвращению использования криптовалюты для облегчения совершения преступлений. Важно разработать надежный комплекс методов профилактики и проведения расследований, которые могут быть адаптированы к изменениям технологий и различным применениям криптовалют, для сведения к минимуму угроз, связанных с их преступным использованием.

B. Технологии и рынки даркнета, включая рынки наркотических средств

14. Интернет открывает новые возможности для незаконной продажи и покупки товаров как через чистую сеть, так и через теневую сеть. В отличие от чистой сети (также называемой поверхностной сетью), под которой понимается информация, размещаемая в открытом доступе и индексируемая общедоступными поисковыми системами, теневая сеть (или даркнет/темные сети; ниже эти термины используются как взаимозаменяемые) состоит из темных сетей с шифрованием, что позволяет владельцу сайта и пользователям сохранить относительную анонимность и препятствует их отслеживанию[23].

15. Рынки даркнета (также именуемые крипторынками)[24] обеспечивают анонимность покупателей и продавцов и в большинстве случаев предполагают использование для оплаты той или иной криптовалюты с целью облегчить продажу таких товаров, как оружие и запрещенные наркотики, и торговлю ими.

16. Согласно информации Агентства Европейского союза по сотрудничеству правоохранительных органов (Европол), рассекреченные персональные, медицинские и финансовые данные являются одним из основных товаров на рынках даркнета и играют решающую роль в таких видах деятельности, как мошенничество, фишинг, хищение личных данных и захват счетов. Тем не менее, хотя на рынках даркнета продается целый ряд контрафактных и пиратских товаров, незаконная торговля в большинстве случаев по-прежнему осуществляется в поверхностной сети[25]. Практика договорных матчей и азартные игры все чаще используются в теневой сети, прежде всего транснациональными организованными преступными группами, в целях создания маршрутов отмывания денег[26]. Участники Европейского регионального подготовительного совещания к четырнадцатому Конгрессу также подчеркнули необходимость бороться с использованием даркнета для совершения преступлений на почве ненависти[27].

17. В отношении наркотических средств во *Всемирном докладе о наркотиках, 2019 год* было отмечено, что в долгосрочном плане закупки таких средств в даркнете растут, хотя в период с 2018 по 2019 год они могли сократиться. Данные Глобального обзора по проблеме наркотиков за 2019 год свидетельствуют о том, что приобретение наркотических средств через даркнет по-прежнему

[22] United Nations Office on Drugs and Crime (UNODC), “UNODC launches training to tackle cryptocurrency-enabled organized crime”, 8 May 2017.

[23] Darren Guccione, “What is the dark web? How to access it and what you'll find”, *The State of Cybersecurity*, 4 July 2019.

[24] Julian Broseus and others, “Studying illicit drug trafficking on Darknet markets: structure and organization from a Canadian perspective”, *Forensic Science International*, vol. 264, 5 March 2016, p. 7.

[25] European Union Agency for Law Enforcement Cooperation (Europol), European Cybercrime entre, *Internet Organised Crime Threat Assessment (IOCTA) 2018* (The Hague, 2018), p. 49.

[26] Robin Cartwright and France Cleland Bones, *Transnational Organized Crime and the Impact on the Private Sector: The Hidden Battalions* (Geneva, Global Initiative against Transnational Organized Crime, 2017), p. 29.

[27] См. A/CONF.234/RPM.5/1, пункт 36 (g).

представляет собой совсем новое явление: 48 процентов лиц, сообщивших о покупке наркотиков через даркнет в 2019 году, начали использовать даркнет для таких целей в предыдущие два года, а еще 29 процентов использовали его в течение двух предшествующих лет[28].

18. Рынки наркотических средств в даркнете могут дать толчок к изменению схем и распространенности употребления наркотиков[29], поскольку они способны снизить определенные риски для покупателей и продавцов, такие как столкновения с применением насилия в районах продажи наркотиков[30], принуждение и арест[31]. Вместе с тем продажа наркотических средств через интернет имеет свои риски. Наибольшие риски могут возникать при совершении соответствующих действий вне сети[32]. Продажа наркотических средств через интернет также может быть связана с увеличением количества случаев передозировки в той мере, в какой она облегчает проведение экспериментов с наркотиками и повышает доступность сильнодействующих наркотических средств[33].

19. В деле ликвидации крупных рынков даркнета достигнуты заметные успехи. Тем не менее, по данным Европола, преступники изучают альтернативные способы обхода действий правоохранительных органов. Новой тенденцией является возникновение бизнес-моделей, в которых преступники действуют под разными именами на основе использования нескольких профилей на разных онлайновых платформах, что в свою очередь обеспечивает возможности для проведения операций разными лицами, а не одним человеком[34].

20. При проведении расследований в теневой сети возникает ряд проблем. Основная проблема заключается в том, что информация в даркнете не индексируется, поэтому следователям нелегко найти соответствующие сведения с помощью поисковых систем или ключевых слов. Кроме того, преступники используют децентрализованные платформы для размещения своих веб-серверов, что создает условия для распространения услуг, выявление которых может быть сопряжено с бóльшими трудностями[35].

21. С другой стороны, правоохранительные органы располагают возможностями для мониторинга рынков даркнета и проведения онлайновых расследований[36]. В этом контексте обеспечить решение проблем может целый ряд инструментов, в том числе поисковые роботы, которые могут использоваться для автоматизации процесса индексации сетевых данных на периодической основе, инструменты извлечения информации для проведения поиска в огромных наборах данных, инструменты анализа криптовалют, предназначенные для отслеживания

[28] *Всемирный доклад о наркотиках, 2019 год: Глобальный обзор спроса на наркотики и их предложения* (издание Организации Объединенных Наций, в продаже под № R.19.XI.8 (брошюра 2)).

[29] Judith Aldridge and David Décary-Hétu, “Hidden wholesale: the drug diffusing capacity of online drug cryptomarkets”, *International Journal of Drug Policy*, vol. 35, September 2016, p. 12.

[30] Julia Buxton and Tim Bingham, *The Rise and Challenge of Dark Net Drug Markets*, Policy brief, No. 7 (Swansea, United Kingdom, Global Drug Policy Observatory, January 2015), pp. 1–24.

[31] Buxton and Bingham, *The Rise and Challenge of Dark Net Drug Markets*. См. также David Décary-Hétu, Masarah Paquet-Clouston and Judith Aldridge, “Going international? Risk taking by cryptomarket drug vendors”, *International Journal of Drug Policy*, vol. 35, September 2016, p. 71.

[32] Judith Aldridge and Rebecca Askew, “Delivery dilemmas: how drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement”, *International Journal of Drug Policy*, vol. 41, March 2017, pp. 101–109.

[33] Nathaniel Popper, “Opioid dealers embrace the dark web to send deadly drugs by mail”, *New York Times*, 10 June 2017.

[34] Europol, European Cybercrime Centre, *Internet Organised Crime Threat Assessment (IOCTA) 2019* (The Hague, 2019), p. 45.

[35] International Criminal Police Organization (INTERPOL) “Innovation report: anonymous networks and darknet” (September 2018), pp. 12–13.

[36] European Monitoring Centre for Drugs and Drug Addiction and Europol, *Drugs and the Darknet: Perspectives for Enforcement, Research and Policy* (Luxembourg, 2017), p. 60 ff.

цепочки платежей, и программные средства технологий распределенного реестра, используемые для поиска улик[37]. Большое значение имеет техническая помощь, и УНП ООН предпринимает активные усилия по организации учебных мероприятий, посвященных методам проведения расследований в теневой сети.

C. Огнестрельное оружие: угрозы безопасности, связанные с технологиями

1. Технополимеры в изготовлении огнестрельного оружия

22. Промышленные полимеры неизбежно будут играть все более доминирующую роль в военной промышленности, создавая проблемы для эффективного осуществления положений об отслеживании и учете огнестрельного оружия, содержащихся в Протоколе против незаконного изготовления и оборота огнестрельного оружия, его составных частей и компонентов, а также боеприпасов к нему, дополняющем Конвенцию Организации Объединенных Наций против транснациональной организованной преступности. Появление промышленных полимеров ставит под угрозу способность компетентных органов надлежащим образом выявлять и расследовать соответствующие преступления и осуществлять судебное преследование лиц, которые их совершают.

23. Модульный комплект по вопросам осуществления контроля за стрелковым оружием (MOSAIC) — сборник примеров рекомендуемой практики в области контроля за стрелковым оружием, не предполагающей обязательного применения, который основан на своде соответствующих международных документов: Протоколе об огнестрельном оружии, Программе действий по стрелковому оружию и связанном с ней Международном документе по отслеживанию и Договоре о торговле оружием, — может помочь странам в решении проблем, возникающих в связи с полимерными рамами и ствольными коробками.

2. Оружие модульной конструкции

24. Новые технологии и существующие лазейки в законодательстве привели к наводнению законных и незаконных рынков комплектами для модификации, преобразования и изготовления соответствующих средств, которые позволяют владельцам оружия при наличии минимальных технических знаний вносить изменения в свое огнестрельное оружие или даже производить полнофункциональные боевые средства.

25. Протокол об огнестрельном оружии применяется к «составным частям и компонентам», однако его требования в отношении маркировки (статья 8) применимы только к «огнестрельному оружию». Это может создавать особые сложности, когда речь идет об оружии модульной конструкции[38]. Для решения данной проблемы могут потребоваться такие меры, как установление контрольного компонента для всех видов огнестрельного оружия, будь то стандартной или модульной конструкции, для целей маркировки, ведения учета и отслеживания; определение данных, которые должны быть указаны на контрольном компоненте, во избежание дублирования серийных номеров; и предоставление инструкций по уникальной идентификации для целей отслеживания, в частности в отношении оружия модульной конструкции[39].

---

[37] INTERPOL, “Innovation report”, p. 14. См. также Shira Stein, “Law enforcement adapts to using cryptocurrency to catch criminals”, *Securities Regulation and Law Report*, 49 SRLR 1029 (Arlington, Virginia, Bureau of National Affairs, 2017).

[38] Giacomo Persi Paoli, “From firearms to weapon systems: challenges and implications of modular design for marking, record-keeping, and tracing”, в: *Behind the Curve: New Technologies, New Control Challenges*, Occasional paper of the Small Arms Survey, No. 32, Benjamin King and Glenn McDonald, eds. (Geneva, Small Arms Survey, 2015), p. 23.

[39] Ibid., p. 40.

3. Технология послойного синтеза (3D-печать)

26. Технология послойного синтеза, в разговорной речи называемая трехмерной или 3D-печатью, является новой технологией, которая может иметь последствия для обеспечения безопасности на местном, национальном и международном уровнях в ближайшей и долгосрочной перспективе. Развитие и распространение технологии послойного синтеза может значительно ускорить распространение оружия и иметь драматические последствия для повседневного совершения преступлений. Кроме того, получение огнестрельного оружия с помощью трехмерной печати может негативно влиять на эффективность схем регистрации и лицензирования огнестрельного оружия и баллистических баз данных, используемых для проведения полицейских расследований.

27. Статья 3 (d) и пункт 1 (a) статьи 5 Протокола об огнестрельном оружии, касающиеся незаконного изготовления огнестрельного оружия, будут применяться к огнестрельному оружию, изготовленному методом трехмерной печати, точно так же, как они применяются к огнестрельному оружию, изготовленному традиционным способом. При этом, однако, скачивание цифровых файлов для трехмерной печати огнестрельного оружия, как представляется, выходит за рамки сферы действия Протокола, что требует принятия срочных законодательных мер.

28. Многие действующие законы и правонарушения, касающиеся изготовления, создания и хранения огнестрельного оружия в отсутствие лицензии, охватывают огнестрельное оружие, полученное методом трехмерной печати, но не всегда включают хранение или распространение проектных файлов[40]. В законах, направленных на пресечение нелегального изготовления огнестрельного оружия, возможно, потребуется установить ответственность третьих сторон в случаях предоставления оборудования в распоряжение лиц, которые могут пожелать изготовить огнестрельное оружие с использованием методов послойного синтеза[41].

29. Комплексный подход к регулированию должен охватывать национальных и международных субъектов, а также государственный и частный секторы. Потенциал двойного применения технологии послойного синтеза не позволяет ограничить ее распространение без одновременного сокращения ее многочисленных преимуществ[42]. Как и в случае с любой новой технологией, важно будет принять меры по организации подготовки и обучения сотрудников правоохранительных органов.

4. Незаконный оборот огнестрельного оружия в теневой сети

30. Теневая сеть может стать предпочтительной платформой для организованных преступных групп и отдельных лиц, желающих приобрести огнестрельное оружие анонимно или в незаконных целях[43]. В ответ на исследование, представленное Управлением Организации Объединенных Наций по вопросам разоружения Первому комитету Генеральной Ассамблеи в 2018 году на основе более крупного исследовательского проекта, реализованного RAND Europe в 2017 году[44], было отмечено, что существует острая необходимость в новых

[40] INTERPOL Innovation Paper, “3D and 4D printing”, INTERPOL Global Complex for Innovation, 2018, p. 6.

[41] N. R. Jenzen-Jones, “Small arms and additive manufacturing: An assessment of 3D-printed firearms, components, and accessories”, в: *Behind the Curve: New Technologies, New Control Challenges*, Occasional paper of the Small Arms Survey, No. 32, Benjamin King and Glenn McDonald, eds. (Geneva, Small Arms Survey, 2015), p. 63–64.

[42] Trevor Johnston, Troy D. Smith and J. Luke Irwin, “Additive manufacturing in 2040: powerful enabler, disruptive threat”, document No. PE-283-RC (Santa Monica, California, RAND Corporation, 2018), p. 17.

[43] RAND Europe, “International arms trade on the dark web” (2019), Findings section, para. 8.

[44] Giacomo Persi Paoli and others, *Behind the Curtain: The Illicit Trade of Firearms, Explosives and Ammunition on the Dark Web* (Santa Monica, California, RAND Corporation, 2017).

формах международного сотрудничества для борьбы с незаконной продажей оружия, которая стала возможной благодаря анонимности теневой сети[45].

31. Доля продаж оружия, которые происходят в теневой сети, как представляется, меньше доли продаж других незаконных товаров[46]. Недавнее исследование, в котором рассматривались только объявления о продаже оружия в теневой сети, показало, что наиболее распространенными являются объявления о продаже огнестрельного оружия, составляющие 42 процента всех объявлений в теневой сети, за которыми следуют цифровые продукты, связанные с оружием (27 процентов), и другие продукты, такие как боеприпасы (22 процента)[47].

32. Понимание масштабов и сферы охвата незаконной торговли оружием в теневой сети имеет ключевое значение для получения более четкого представления о серьезности угрозы и последствиях для правоохранительных органов. На национальном уровне директивные структуры должны принять меры к тому, чтобы правоохранительные органы были надлежащим образом укомплектованы кадрами, подготовлены и оснащены для решения соответствующих проблем. Действующие международно-правовые рамки, в частности Конвенция об организованной преступности и дополняющий ее Протокол об огнестрельном оружии, могут обеспечить основу для комплексных подходов к борьбе с данным явлением. Необходимо провести всесторонний анализ вопроса о применимости существующих правил проведения брокерских операций (посреднической деятельности), предусмотренных Протоколом об огнестрельном оружии (статья 15) и Договором о торговле оружием (статья 10)[48].

5. Автономное оружие летального действия

33. Хотя существование полностью автономного оружия официально не признается, идея использования искусственного интеллекта для контроля над такими вооружениями вызвала бурные дебаты. В 2016 году пятая Конференция Высоких Договаривающихся Сторон Конвенции о запрещении или ограничении применения конкретных видов обычного оружия, которые могут считаться наносящими чрезмерные повреждения или имеющими неизбирательное действие, по рассмотрению действия Конвенции учредила Группу правительственных экспертов по вопросам, касающимся новых технологий в сфере создания смертоносных автономных систем вооружений. На своей сессии 2019 года Группа рекомендовала Высоким Договаривающимся Сторонам одобрить руководящие принципы, подтвержденные Группой[49].

D. Торговля людьми

34. Исследования последних лет и прямые доказательства свидетельствуют о том, что торговцы людьми используют технологии на всех этапах совершения преступления, включая вербовку, контроль и эксплуатацию жертв.

35. Одна из причин, по которым торговцы людьми используют технологии, заключается в том, что технологии дают им возможность действовать анонимно и скрывать свою личность. Кроме того, криптовалюта позволяет торговцам людьми осуществлять финансовые операции и анонимно перемещать доходы от преступной деятельности. Еще одна причина состоит в том, что технологии

---

[45] Giacomo Persi Paoli, *The Trade in Small Arms and Light Weapons on the Dark Web*, United Nations Office for Disarmament Affairs (UNODA) Occasional Papers, No. 32 (United Nations publications, Sales No. E.19.XI.1), p. ix.

[46] Damien Rhumorbarbe and others, “Characterising the online weapons trafficking on cryptomarkets”, *Forensic Science International*, vol. 283, December 2018, pp. 16–20.

[47] RAND Europe, “International arms trade on the dark web” (2019), Findings section, para. 4.

[48] Simonetta Grassi and Mareike Buettner, “Annex: overview of international legal instruments and their applicability to illicit firearms trafficking on the dark web”, в: Paoli and others, *Behind the Curtain*, p. 101.

[49] CCW/GGE.1/2019/3, приложение IV.

облегчают вербовку и эксплуатацию жертв торговцами людьми. Онлайновая рубричная реклама и сайты социальных сетей могут использоваться в качестве «каналов для торговли людьми»[50].

36. Далее следует отметить, что противоправное использование технологий может упрощать для торговцев людьми заключение сделок с пользователями, выход на новые рынки и расширение преступных операций. Лица, занимающиеся торговлей людьми, могут использовать потоковое вещание для выхода на более широкий рынок потребителей, которые могут вообще не иметь физического контакта с жертвой[51].

37. Кроме того, противоправное использование технологий может помогать торговцам людьми контролировать жертв и принуждать их к совершению определенных действий. Для облегчения эксплуатации жертв торговцы людьми могут применять систему отслеживания местонахождения. Даже тех пострадавших, которым удалось ускользнуть, можно отследить: злоумышленники узнают, где они прячутся, используя трекеры местонахождения на их мобильных телефонах.

38. В то же время правоохранительные органы используют систему отслеживания местонахождения для выяснения места пребывания лиц, подозреваемых в торговле людьми, или иных лиц, входящих в сеть такой торговли. Применение данных об отслеживании местонахождения, полученных пострадавшими, является другой стороной медали, учитывая тот факт, что жертвы могут рассматриваться как «ходячие базы подтверждающих данных»[52].

39. Для использования технологических мер в борьбе с торговлей людьми необходимо сотрудничество между секторами. Индустрия информационно-коммуникационных технологий и международные организации наладили партнерские отношения в целях изучения возможностей использования технологий для предупреждения торговли людьми и содействия реабилитации жертв. Коалиция «Технологические компании против торговли людьми» (Tech Against Trafficking), в состав которой входят ведущие технологические компании, научные учреждения и Международная организация по миграции, представляет перечень технологических решений, применяемых для борьбы с торговлей людьми[53].

40. Наращивание потенциала всех участвующих сторон имеет ключевое значение для решения проблем, связанных с использованием технологий в целях торговли людьми. Необходимо тщательно продумать вопросы разработки, использования, сохранения, мониторинга и оценки технологий, применяемых специалистами-практиками для борьбы с торговлей людьми[54]. При этом разработчики соответствующего инструментария должны предвидеть и учитывать различия между пользователями, которые могут стать жертвами торговли людьми[55].

---

[50] Mark Latonero, *Human Trafficking Online: The Role of Social Networking Sites and Online Classifieds*, Centre on Communication Leadership and Policy Research Series (Los Angeles, University of Southern California, September 2011), p. 8.

[51] Inter-Agency Coordination Group against Trafficking in Persons, “Human trafficking and technology: trends, challenges and opportunities”, Issue brief, No. 7 (2019), pp. 1–2.

[52] Felicity Gerry, Julia Muraszkiewicz and Niovi Vavoula, “The role of technology in the fight against human trafficking: reflections on privacy and data protection concerns”, *Computer Law and Security Review*, vol. 32, No. 2 (April 2016), pp. 210–211.

[53] Business for Social Responsibility, “List of technology tools and initiatives identified by tech against trafficking”, 15 January 2019.

[54] Inter-Agency Coordination Group against Trafficking in Persons, “Human trafficking and technology”, p. 4.

[55] См. Mark Latonero, Bronwyn Wex and Meredith Dank, *Technology and Labor Trafficking in a Networked Society: General Overview, Emerging Innovations, and Philippines Case Study* (Los Angeles, University of Southern California, Annenberg Center on Communication Leadership and Policy, 2015), p. 11.

E. Незаконный ввоз мигрантов

41. Информационно-коммуникационные технологии стали важным инструментом, который широко используется мигрантами и вербовщиками для передачи информации о маршрутах, услугах и ценах[56]. Кроме того, социальные сети расширяют возможности лиц, занимающихся незаконным ввозом мигрантов, помогая им менять маршруты в ответ на действия правоохранительных органов в странах транзита и тем самым повышая эффективность операций по незаконному ввозу и одновременно затрудняя проведение расследований и судебного преследования в связи с такими преступлениями[57].

42. Стремительное развитие мобильных технологий может иметь последствия для отношений между мигрантами и лицами, занимающимися их незаконным ввозом. В нескольких группах сети Facebook мигранты могут проверить надежность конкретных организаторов незаконного ввоза и поделиться информацией о том, с кем лучше всего связаться. Эта система определяется как «иерархия доверия»[58].

43. Технологии также могут использоваться для финансовых платежей, поскольку оплата услуг лиц, занимающихся незаконным ввозом мигрантов, осуществляется главным образом через онлайновые платежные системы. Криптовалюты могут упрощать для этих лиц получение, сокрытие и перемещение денежных средств. Такие валюты могут способствовать отмыванию денег и помогать организаторам незаконного ввоза мигрантов избежать расследования и задержания посредством обеспечения анонимности и уменьшения необходимости перевозить большие количества наличности.

44. Технологии также играют важную роль в обеспечении поддельных документов на выезд или удостоверений личности, которые облегчают незаконный ввоз мигрантов. В целях создания или копирования паспортов либо внесения в них тех или иных изменений мошенники используют разные виды оборудования. В некоторых случаях для создания первоклассных подделок (паспортов «зеркального качества») применяются высокотехнологичные инструменты[59].

45. Вместе с тем технологические инновации можно рассматривать под разными углами, а не только с позиции выгод для лиц, занимающихся незаконным ввозом мигрантов. Внедрение цифровых технологий также сокращает информационные пробелы, обеспечивающие возможности для успешной деятельности таких лиц. Интернет можно использовать для оказания мигрантам помощи в подключении к социальным сетям, предоставляющим поддержку и информацию. Недавняя тенденция, обусловленная технологическим прогрессом, заключается в том, что растущее число мигрантов действует самостоятельно на протяжении всего миграционного процесса и в меньшей степени зависит от лиц, занимающихся их незаконным ввозом. Это повышает автономность мигрантов и уменьшает их уязвимость перед эксплуатацией[60].

46. Использование мигрантами социальных сетей зависит от их национальности, этнической принадлежности, региона происхождения и образования,

---

[56] Europol and INTERPOL, “Migrant smuggling networks: executive summary” (May 2016), p. 8.

[57] CTOC/COP/WG.7/2018/2, пункт 25.

[58] Judith Zijlstra and Ilse van Liempt, “Smart(phone) travelling: understanding the use and impact of mobile technology on irregular migration journeys”, *International Journal of Migration and Border Studies*, vol. 3, Nos. 2 and 3 (March 2017), pp. 176–177.

[59] UNODC Regional Office for South-East Asia and the Pacific, *Facilitators of Smuggling of Migrants in Southeast Asia: Fraudulent Documents, Money Laundering, and Corruption* (Bangkok, 2019), p. 26.

[60] UNODC, Doha Declaration, Tertiary, Education for Justice University Module Series, Trafficking in Persons and Smuggling of Migrants, “Module 14: links between cybercrime, trafficking in persons and smuggling of migrants–technology in smuggling of migrants”. Доступно по адресу: www.unodc.org/e4j/.

а также от имеющегося у них доступа к интернету[61]. Имеющиеся данные свидетельствуют о наличии цифрового разрыва между группами мигрантов, который обусловлен неравенством в физическом доступе к цифровым технологиям и их использовании, в навыках, необходимых для эффективного применения различных технологий, и в способности оплачивать соответствующие услуги[62].

47. В аспекте охраны правопорядка растет интерес к поиску способов использования технологий для пресечения деятельности сетей незаконного ввоза мигрантов. Кроме того, доказательства, полученные в социальных сетях и/или с помощью технологий, могут подкреплять показания незаконно ввезенных мигрантов в ходе соответствующих уголовных разбирательств.

48. Надлежащее использование технологий помогает правительствам, частному сектору и неправительственным организациям в рамках их соответствующих сфер компетенции предотвращать незаконный ввоз мигрантов и уменьшать его масштабы. В связи с этим крайне важно повышать эффективность мер уголовного правосудия и создавать стимулы и партнерства с поставщиками интернет-услуг в целях совершенствования методов мониторинга и выявления контента, имеющего отношение к незаконному ввозу, и представления соответствующих сведений.

F. Надругательство над детьми и их эксплуатация в сети

49. Сексуальные надругательства над детьми и их эксплуатация имели место до появления интернета, однако онлайновый аспект этих преступлений позволяет преступникам взаимодействовать друг с другом и получать материалы о сексуальной эксплуатации детей по сети. Кроме того, увеличение числа детей младшего возраста, имеющих доступ к интернету, упрощает для преступников установление контакта с детьми по сравнению с тем, как это происходит в реальности, что в свою очередь оказывает значительное влияние на способы совершения соответствующих преступлений.

50. Технологические достижения стали играть важную роль в сексуальной эксплуатации детей в коммерческих целях. Клиенты индустрии детского секс-туризма могут использовать облачную обработку данных для хранения фотографий или видеозаписей, избегая таким образом рисков, связанных с физической транспортировкой материалов о сексуальной эксплуатации детей. Кроме того, технология мобильной телефонии связывает организаторов сексуальной эксплуатации и надругательств над детьми, их жертв и потребителей соответствующих услуг, уменьшая тем самым необходимость физического присутствия производителей и распространителей материалов при заключении сделок, что в свою очередь сокращает возможности их обнаружения.

51. К числу основных форм надругательств над детьми и их эксплуатации, которым способствуют информационно-коммуникационные технологии, относятся вовлечение в порнографическую деятельность и вхождение в доверие (груминг) и нежелательные сексуальные домогательства в сети, причем многие из таких актов эксплуатации связаны с совершением неприемлемых сексуальных действий с детьми. Исследование УНП ООН по данному вопросу акцентирует внимание на новых формах надругательств над детьми и их эксплуатации, таких как контент, создаваемый пользователями, самогенерируемый контент,

[61] European Commission, “The use of social media in the fight against migrant smuggling”, European Migration Network (EMN) Inform (September 2016).

[62] Alam Khorshed and Sophia Imran, “The digital divide and social inclusion among refugee migrants: a case in regional Australia”, *Information Technology and People*, vol. 28, No. 2 (June 2015), pp. 344 ff.

включая секстинг, прямая трансляция сцен сексуального надругательства и созданные на заказ материалы о сексуальных надругательствах над детьми[63].

52. По данным Европола, прямая трансляция сцен сексуальных надругательств превратилась в постоянную угрозу и осуществляется через приложения для социальных сетей и видеочатов, игровые платформы и чат-комнаты в интернете. Кроме того, по всей видимости, имеет место переход от использования компьютеров к использованию смартфонов и планшетов, а также от кабельного интернета к технологии Wi-Fi и мобильному интернету[64].

53. Одной из наиболее значимых угроз при распространении материалов о сексуальной эксплуатации детей в сети является непрерывное увеличение использования даркнета. Согласно данным Фонда по наблюдению за использованием интернета, наличие замаскированных веб-сайтов, использующих метод «цифрового пути» для сокрытия изображений сцен сексуального надругательства над детьми, по-прежнему является серьезной проблемой. При этом в последние годы Фонд отмечал неуклонный рост количества веб-адресов, по которым размещаются материалы о сексуальных надругательствах над детьми: с 68 092 в 2015 году до 105 047 в 2018 году[65].

54. Кроме того, при получении более сложных технических средств лица, совершающие сексуальные преступления в отношении детей в сети, продолжат искать новые способы действий, позволяющие избежать обнаружения. В последнее время отмечается переход от крупных форумов к созданию небольших групп пользователей с помощью мобильных приложений для обмена сообщениями со сквозным шифрованием.

55. Отсутствие в ряде стран применимых правовых норм, определяющих порядок действий в связи с новыми формами надругательств над детьми, и различия в законах, защищающих детей и устанавливающих возраст согласия, создают значительные проблемы и снижают вероятность успешного выявления и расследования преступлений и судебного преследования за их совершение.

56. Технологии также могут обеспечить правоохранительным органам способы борьбы с сопутствующими проблемами[66]. Инновации в таких методах и приемах, как извлечение информации и аналитическая обработка данных, оптимизируют процессы криминалистической экспертизы для продвижения расследований. Методы, предусматривающие использование информационных технологий, должны применяться при соблюдении границ защиты прав человека в связи с травмирующим характером сексуальной эксплуатации детей и возрастом, а также уязвимостью детей-свидетелей.

57. Кроме того, были созданы базы данных для загрузки материалов о сексуальных надругательствах над детьми в целях проведения расследований, такие как Международная база данных о сексуальной эксплуатации детей, сформированная Международной организацией уголовной полиции. В Соединенных Штатах Америки база данных Национального центра по делам пропавших и эксплуатируемых детей служит центральным хранилищем материалов о сексуальных надругательствах над детьми[67].

58. Эффективные действия по борьбе с надругательствами и эксплуатацией в отношении детей с помощью информационно-коммуникационных технологий

---

[63] UNODC, *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children* (Vienna, 2015), pp. 21 ff.

[64] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2018*, p. 35.

[65] Internet Watch Foundation, *Once Upon a Year* (Cambridge, United Kingdom, 2018), pp. 19 and 43.

[66] Victoria Brains, “Online child sexual exploitation: towards an optimal international response”, *SSRN Electronic Journal*, 29 August 2018.

[67] UNODC, Doha Declaration, Tertiary, Education for Justice University Module Series, Cybercrime, “Module 12: interpersonal cybercrime–online child sexual exploitation and abuse”. Доступно по адресу: www.unodc.org/e4j/.

требуют многостороннего подхода, предусматривающего охват и активное привлечение к участию в проводимых мероприятиях детей, семей, общин, правительств, гражданского общества и частного сектора[68].

G. Искусственный интеллект и робототехника

59. На этапе после третьей промышленной революции, вызванной появлением интернета и мобильных технологий, технологии искусственного интеллекта на основе больших данных[69] создают условия для четвертой промышленной революции. Хотя это может способствовать глобальному развитию и преобразованиям в обществе, содействуя достижению целей в области устойчивого развития, в данном контексте также возникают правовые, этические и социальные проблемы и вызовы. В сфере охраны правопорядка достижения в области искусственного интеллекта могут создавать не только возможности, но и риски, в связи с чем необходимы стратегический подход и инвестиции в усилия и ресурсы[70].

60. Почти на всех региональных подготовительных совещаниях к четырнадцатому Конгрессу подчеркивались необходимость и важность изучения путей и способов обеспечения работникам уголовного правосудия и правоохранительных органов возможности с максимальной отдачей использовать развивающиеся технологии, такие как искусственный интеллект и информационно-коммуникационные технологии, включая большие данные, в борьбе с преступностью[71].

61. Обсуждаются, в частности, такие вопросы, как использование искусственного интеллекта для проведения виртуальной аутопсии; системы прогнозирования преступлений, предназначенные для оказания полиции помощи в оптимизации ресурсов; инструментарий для выявления тех или иных форм поведения; подходы к отслеживанию, основанные на технологиях распределенного реестра и предусматривающие соблюдение конфиденциальности; и автономные патрульные машины[72]. Кроме того, все больше правоохранительных органов, с удовлетворением отмечая прогресс в области искусственного интеллекта, делающий роботов «умнее» и позволяющий им заменить человека в выполнении многих функций и задач, применяют соответствующие технологические достижения при проведении различных операций. Уровень использования робототехники далеко не однороден, поскольку некоторые страны добились бóльших успехов в исследовании и применении таких технологий в сравнении с другими странами[73].

62. Как представляется, искусственный интеллект и машинное обучение обеспечивают все более эффективную защиту от отмывания денег. Как и алгоритмы, помогающие интернет-магазинам розничной торговли определять целевых клиентов, искусственный интеллект и машинное обучение могут способствовать применению более продуманной и точной политики должной осмотрительности на основе интерпретации сигналов, указывающих на преступную деятельность, и анализа гораздо больших объемов данных с большей надежностью. Кроме того, платформы социальных сетей все чаще используют машинное обучение для блокирования незаконного контента и фальшивых новостей. Предприятия

---

[68] UNODC, *Study on the Effects of New Information Technologies*.

[69] Victor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution that Will Transform How We Live Work and Think* (London, John Murray, 2013).

[70] Межрегиональный научно-исследовательский институт Организации Объединенных Наций по вопросам преступности и правосудия (ЮНИКРИ) создал в Гааге Центр искусственного интеллекта и робототехники, который будет служить международным ресурсом по вопросам, связанным с искусственным интеллектом и робототехникой.

[71] A/CONF.234/RPM.1/1, пункт 61 (j); A/CONF.234/RPM.2/1, пункт 79 (k); A/CONF.234/RPM.3/1, пункт 56 (f); и A/CONF.234/RPM.4/1, пункт 57 (e).

[72] INTERPOL and UNICRI, “Artificial intelligence and robotics for law enforcement” (Turin, Italy, 2019), p. v.

[73] Ibid., p. 6.

используют искусственный интеллект для управления повышенными рисками и оперативного выявления случаев мошенничества в целях предотвращения и прогнозирования преступлений.

63. Вместе с тем искусственный интеллект — это во многих смыслах палка о двух концах, поскольку он может значительно изменить подход правоохранительных органов к задаче поддержания общественного порядка, совершенствуя при этом методы работы преступных и террористических групп и даже способствуя появлению новых форм преступности[74]. В обобщенном виде приоритетная задача деятельности, которую можно красноречиво охарактеризовать как борьбу по принципу «выживает сильнейший»[75], формулируется следующим образом: содействие охране правопорядка с использованием искусственного интеллекта в целях борьбы с преступлениями, совершаемыми на его основе.

H. Международное сотрудничество по уголовно-правовым вопросам и использование технологий

64. В настоящее время в области международного сотрудничества по уголовно-правовым вопросам ведется дискуссия о том, каким образом центральные органы власти могут в полной мере воспользоваться преимуществами современных технологий. В политическом плане в 2016 году Конференция участников Конвенции Организации Объединенных Наций против транснациональной организованной преступности призвала государства-участники в полной мере и наиболее эффективно использовать имеющиеся технологии для содействия сотрудничеству между центральными органами[76].

65. Удовлетворение растущей потребности в расширении международного сотрудничества зависит от наличия ресурсов, включая «технологические ресурсы», такие как сети для безопасной передачи информации, оборудование, облегчающее коммуникацию (например, теле- и видеоконференции), и системы организации рассмотрения дел для отслеживания входящих и исходящих запросов. Растущая потребность в ресурсах также может быть связана с повышением эффективности обработки просьб об оказании взаимной правовой помощи, включающих электронные доказательства (например, за счет создания специализированных подразделений в рамках центральных органов).

66. Очевидно, что организация рассмотрения дел в центральных органах отражает прогресс, достижения или недостатки во всех институциональных механизмах уголовного правосудия государств-членов в зависимости от различий в их потенциале. Во многих странах, где учетные записи по-прежнему ведутся на бумажных носителях, поиск таких записей и предоставление соответствующих документов запрашивающей стране могут оказаться весьма непростой задачей. В странах, находящихся на другом конце спектра, современные технологии позволяют использовать электронные платформы для управления входящими и исходящими просьбами об оказании взаимной правовой помощи или сбора статистических данных о делах и тенденциях[77].

---

[74] В докладе за 2018 год рассматривается преступное использование искусственного интеллекта и определяются три основные категории сопутствующих угроз: a) угрозы, связанные с цифровой безопасностью; b) угрозы, связанные с физической безопасностью; и c) угрозы, касающиеся политической безопасности (распространение фальшивых новостей и автоматизированная дезинформация или организация кампаний с целью повлиять на поведение при голосовании и, возможно, подорвать способность вести честные общественные дискуссии). См. Miles Brundage and others, *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation* (February 2018).

[75] INTERPOL Innovation Paper, “Artificial intelligence”, INTERPOL Global Complex for Innovation, 2018, p. 2.

[76] Резолюция 8/1 Конференции.

[77] Asian Development Bank and Organization for Economic Cooperation and Development, *Mutual Legal Assistance in Asia and the Pacific: Experiences in 31 Jurisdictions* (2017), p. 31.

67. Что касается передачи просьб об оказании взаимной правовой помощи, то участники Регионального подготовительного совещания стран Латинской Америки и Карибского бассейна к четырнадцатому Конгрессу обсудили вопрос об использовании для этой цели электронных средств, которое было отмечено в качестве положительной практики в некоторых странах данного региона[78]. Они рекомендовали содействовать использованию технологий для повышения эффективности международного сотрудничества по уголовно-правовым вопросам, учитывая, в частности, соглашения между центральными органами об электронной передаче просьб о международном сотрудничестве в соответствии с национальным законодательством[79].

68. УНП ООН принимает меры по развитию международного сотрудничества, в том числе с помощью специально разработанных инструментов и технологических инноваций: информационно-справочного портала, известного как «Распространение электронных ресурсов и законов о борьбе с преступностью» (ШЕРЛОК), справочника компетентных национальных органов и переработанной версии Программы составления просьб об оказании взаимной правовой помощи[80].

69. УНП ООН активно поддерживает межправительственные процессы, в рамках которых международное сотрудничество, связанное с электронными доказательствами, стало одним из политических и правовых приоритетов. К числу примеров таких процессов относятся деятельность межправительственной группы экспертов открытого состава для проведения всестороннего исследования проблемы киберпреступности[81], тематическое обсуждение киберпреступности на двадцать седьмой сессии Комиссии по предупреждению преступности и уголовному правосудию, состоявшейся в мае 2018 года[82], и соответствующая деятельность Рабочей группы по вопросам международного сотрудничества Конференции участников Конвенции об организованной преступности.

I. Этические соображения: процедурные и правозащитные гарантии

70. Технологические инструменты могут служить полезными отправными точками в деле устранения угроз, связанных с преступностью. Тем не менее при конкретном применении данных инструментов необходимо проявлять осторожность, чтобы гарантировать их ответственное и этичное использование и избежать нежелательных последствий. Это особенно важно, учитывая тот факт, что многие из нынешних и будущих технологий могут иметь серьезные последствия для неприкосновенности частной жизни и гражданских свобод.

71. Например, программное обеспечение для распознавания лиц используется сотрудниками правоохранительных органов для гораздо более оперативной идентификации подозреваемых. При этом, однако, критики выражают обеспокоенность по поводу того, что соответствующая практика может привести к чрезмерному наблюдению со стороны правительства, корпоративным манипуляциям и нарушению неприкосновенности частной жизни. Кроме того, аспект биометрических систем, связанный с сохранением данных, может поставить под угрозу конфиденциальность ввиду возможности их потенциального неправомерного использования[83].

---

[78] A/CONF.234/RPM.3/1, пункт 72.

[79] Там же, пункт 79 (n).

[80] Доступна по адресу: www.unodc.org/mla/en/index.html.

[81] UNODC, Cybercrime, “Meeting of the IED on cybercrime”. Доступно по адресу: www.unodc.org.

[82] См. руководство для этого тематического обсуждения (E/CN.15/2018/6).

[83] Max Snijder, *Biometrics, Surveillance and Privacy* (Ispra, Italy, European Reference Network for Critical Infrastructure Protection (ERNCIP) Thematic Group Applied Biometrics for the Security of Critical Infrastructure, 2016), pp. 4 ff.

72. Еще одним примером может служить предиктивная полицейская деятельность или аналитика. В последние годы все больше правоохранительных органов внедряют программное обеспечение для анализа статистических данных, выявления связей между различными видами деятельности и делами и даже прогнозирования того, где возникнет следующая угроза. При этом, однако, использование прогностических методов работы полиции для целей профилирования может приводить к стигматизации отдельных лиц и групп и, таким образом, к формам дискриминации на основе тех или иных алгоритмов[84].

73. В области борьбы с торговлей людьми и при изучении взаимосвязи использования технологий с правами человека и защитой данных[85] важно обеспечивать более эффективную защиту жертв. Решения по борьбе с торговлей людьми следует разрабатывать под тщательным контролем, с тем чтобы не допустить нарушения прав на неприкосновенность частной жизни и несправедливого выделения определенных групп[86], обеспечивая и для пострадавших безопасный доступ к технологиям[87].

74. Еще одним важным фактором является соблюдение процессуальных гарантий допустимости в суде доказательств, полученных с помощью специальных методов расследования, включая методы, предусматривающие применение технологий. Использование специальных методов расследования регулируется соответствующими положениями внутреннего законодательства и применимыми многосторонними документами[88]. В большинстве юрисдикций сбор доказательств требует строгого соблюдения гарантий от возможных злоупотреблений полномочиями, включая судебный или независимый надзор за использованием этих методов и соблюдением принципов законности, субсидиарности и соразмерности[89]. Электронные доказательства допустимы при соблюдении установленных процедур[90]. Применение общих принципов внутреннего процессуального законодательства и национальной судебной практики в отношении допустимости доказательств, полученных в ходе судебной экспертизы по делам с использованием криптовалют, является новой и сложной областью, требующей дальнейшего рассмотрения и обмена опытом[91].

75. С расширением использования искусственного интеллекта и робототехники правоохранительными органами возрастает значимость обеспечения его соответствия этическим принципам. Были предприняты инициативы в области «мягкого права» в целях сведения к минимуму рисков нарушения основных прав, вытекающих из использования систем искусственного интеллекта правоохранительными органами, и уменьшения неопределенности в вопросе о

---

[84] См. Eva Schlehahn and others, “Benefits and pitfalls of predictive policing”, в: *2015 European Intelligence and Security Informatics Conference: EISIC 2015*, Joel Brynielsson and Moi Hoon Yap, eds. (Piscataway, New Jersey, Institute of Electrical and Electronics Engineers, Inc, 2015), pp. 145–148; Albert Meijer and Martijn Wessels, “Predictive policing: review of benefits and drawbacks”, *International Journal of Public Administration*, vol. 42, No. 12 (February 2019).

[85] См. Inter-Agency Coordination Group against Trafficking in Persons, “Human trafficking and technology”, p. 5.

[86] Mark Latonero and others, *The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking,* Research Series on Technology and Human Trafficking (November 2012), p. 38.

[87] Gerry, Muraszkiewicz and Vavoula, “The role of technology in the fight against human trafficking”, p. 211.

[88] См. статью 20 Конвенции Организации Объединенных Наций против транснациональной организованной преступности и статью 50 Конвенции Организации Объединенных Наций против коррупции.

[89] Информацию о соответствующей практике Европейского суда по правам человека см. в работе Dimosthenis Chrysikos, “Article 50: special investigative techniques”, в: *The United Nations Convention against Corruption. A Commentary*, Cecily Rose, Michael Kubiciel and Oliver Landwehr, eds., Oxford Commentaries on International Law Series (Oxford, Oxford University Press, 2019), pp. 507 ff.

[90] E/CN.15/2018/6, пункт 30.

[91] Michael Fröwis and others, “Safeguarding the evidential value of forensic cryptocurrency investigations” (2019).

правовой ответственности, связанной с этичным использованием искусственного интеллекта и робототехники в целом[92].

76. Главный вопрос, однако, состоит в том, склонно и готово ли общество в целом к принятию такой практики, как создание разветвленной сети устройств наблюдения, даже если это отвечает интересам обеспечения общественного порядка и безопасности[93]. Решения, касающиеся технологий, должны опираться на широкий общественный диалог о связанных с ними издержках, выгодах и применимых нормах. Вопрос об убеждении общественности в преимуществах технологий в сферах правоохранительной деятельности и уголовного правосудия является частью общей дискуссии, которая должна последовательно проводиться для обеспечения того, чтобы компетентные органы не утратили доверия общин и граждан, которых они обязаны защищать. Данная дискуссия должна отражать и другую сторону медали — критические замечания по поводу того, что возросшая зависимость от технологий также может увеличить зависимость от стратегий принудительного наблюдения и контроля[94].

77. Группа высокого уровня по цифровому сотрудничеству рекомендовала Генеральному секретарю организовать во всех учреждениях обзор применения действующих международных соглашений и стандартов в области прав человека к новым и возникающим цифровым технологиям. Следует предложить гражданскому обществу, правительствам, частному сектору и широкой общественности высказать свое мнение о способах применения существующих документов по правам человека в цифровую эпоху в рамках активного и транспарентного процесса[95].

78. Для поиска решений в тех случаях, когда есть основания полагать, что применение технологий может войти в противоречие с принципом неприкосновенности частной жизни или другими правами человека, необходим сбалансированный подход. Во избежание использования технологий в качестве троянского коня для потенциального нарушения основополагающих прав необходимо постоянно отслеживать развитие технологий и оценивать его влияние.

III. Выводы и рекомендации

79. В духе греческой мифологии проблему можно сформулировать следующим образом: что в конечном счете представляют собой технологии — панацею (лекарство, якобы исцеляющее от всех болезней, названное так в честь дочери Асклепия) для предупреждения преступности или ящик Пандоры, процесс, который, как выясняется, имеет серьезные последствия в плане расширения возможностей для совершения преступлений (как в мифе о Пандоре, открывающей сосуд и выпускающей наружу все беды и несчастья)?

80. Истина лежит посредине, вне манихейских представлений. Технологии неизбежно имеют как положительные, так и отрицательные стороны. Правоохранительные органы и органы уголовного правосудия пользуются технологическими достижениями. В то же время взрыв технологических инноваций создает благодатную почву для расцвета преступности. Характер совершаемых

[92] Институт инженеров по электротехнике и радиоэлектронике (IEEE) опубликовал глобальный трактат по вопросам этики автономных и интеллектуальных систем (этически приемлемого дизайна) для приведения технологий в соответствие с моральными ценностями и этическими принципами. См. IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems* (Pascataway, New Jersey, 2019).

[93] INTERPOL and UNICRI, “Artificial intelligence and robotics for law enforcement”, p. 14.

[94] James Byrne and Gary Marx, “Technological innovations in crime prevention and policing: a review of the research on implementation and impact”, *Cahiers Politiestudies*, vol. 20, No. 3 (2011), p. 30.

[95] United Nations, *The Age of Digital Interdependence: Report of the Secretary-General’s High-level Panel on Digital Cooperation* (June 2019), recommendation 3A.

преступлений кардинально меняется в связи с различными применениями современных технологий, и компетентным органам необходимо принимать меры, чтобы уровень их технической оснащенности был не ниже, чем у преступников.

81. Исход текущего противостояния между преступниками и защитниками правопорядка будет во многом зависеть от вложения средств в подготовку кадров и обеспечения постоянной адаптации стратегий в области предупреждения преступности и уголовного правосудия для решения возникающих проблем с учетом этических соображений и соображений, касающихся прав человека.

82. Четырнадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию, возможно, пожелает рассмотреть следующие рекомендации:

a) государствам-членам следует выявлять и устранять пробелы в своих правовых системах для обеспечения эффективного расследования преступлений, совершаемых с использованием технологий, и судебного преследования за их совершение, в том числе путем принятия новых и/или обновления действующих законов с технически нейтральными формулировками и расширения международного сотрудничества;

b) государствам-членам следует поддерживать и расширять партнерские отношения и взаимодействие с различными заинтересованными сторонами, включая международные и региональные организации, гражданское общество, частный сектор и научные круги, в целях активизации исследований, инновационной деятельности, развития и использования технологий в сферах правоохранительной деятельности и уголовного правосудия;

c) государствам-членам следует выявлять и оценивать риски отмывания денег и финансирования терроризма, возникающие в связи с деятельностью или операциями с участием поставщиков услуг в сфере виртуальных активов; применять подход, основанный на оценке рисков, для обеспечения соразмерности мер по предотвращению или уменьшению масштабов отмывания денег и финансирования терроризма выявленным рискам; и требовать, чтобы поставщики услуг в сфере виртуальных активов выявляли, оценивали и принимали эффективные меры по уменьшению рисков, связанных с отмыванием денег и финансированием терроризма;

d) государствам-членам следует вкладывать больше средств в надлежащую подготовку кадров в целях укрепления потенциала для эффективного решения вопросов, возникающих в связи с использованием криптовалют, в ходе расследований;

e) государствам-членам следует включить в свое законодательство положения, касающиеся хранения, публикации и передачи цифровых материалов, которые могут быть использованы для последующего изготовления огнестрельного оружия, и проводить мероприятия по наращиванию потенциала в целях развития навыков предупреждения, выявления и расследования таких деяний и незаконного оборота огнестрельного оружия в даркнете и судебного преследования виновных;

f) УНП ООН следует и впредь содействовать проведению регулярных совещаний сообществ специалистов-практиков для обеспечения того, чтобы следователи были в курсе новых методов изготовления и передачи огнестрельного оружия и соответствующих методов расследования;

g) государствам-членам следует уделять особое внимание формированию опыта и потенциала компетентных органов во всех соответствующих секторах в целях создания условий для оптимального использования технологий в борьбе с торговлей людьми при одновременной защите прав жертв;

h) УНП ООН следует и далее совершенствовать свои технические руководящие указания для государств-членов и расширять оказываемую им поддержку в целях более эффективного определения и применения основанных на

технологиях мер системы уголовного правосудия по предупреждению и расследованию случаев торговли людьми и незаконного ввоза мигрантов и связанному с ними судебному преследованию;

i) государствам-членам следует принять законодательные или иные меры с целью облегчить выявление поставщиками интернет-услуг и интернет-доступа и другими соответствующими структурами материалов о сексуальной эксплуатации детей и сексуальных надругательствах над ними и обеспечить представление информации о таких материалах и их удаление;

j) государствам-членам следует осуществлять политику и обмениваться передовой практикой, в том числе в отношении программ поддержки жертв и учета гендерной проблематики, в целях защиты детей от сексуальной эксплуатации и сексуальных надругательств;

k) государствам-членам следует добиваться лучшего понимания рисков, создаваемых злонамеренным использованием искусственного интеллекта, и постоянно следить за развитием новых технологий в целях обеспечения готовности, подотчетности, транспарентности и добросовестности; поощрять соблюдение этических норм при использовании этих технологий; и обеспечивать уверенность граждан и общин в правильности их использования и доверия к нему;

l) государствам-членам в сотрудничестве с УНП ООН и другими международными организациями следует содействовать оказанию технической помощи и подготовке кадров в целях повышения квалификации специалистов-практиков и центральных органов в области использования технологий для активизации международного сотрудничества.