Сафронов Никита Сергеевич, студент,
ФКОУ ВО Пермский институт ФСИН России

Научный руководитель:
Кривенцева Светлана Михайловна,
ФКОУ ВО Пермский институт ФСИН России

ПАРАДОКС ТЕМНОЙ ЦИФРЫ: МЕТОДОЛОГИЧЕСКИЕ ПРОБЛЕМЫ ИЗМЕРЕНИЯ ЛАТЕНТНОЙ ПРЕСТУПНОСТИ В ЭПОХУ BIG DATA

Аннотация. Статья посвящена критическому анализу методологических проблем измерения латентной преступности в условиях цифровой трансформации общества и взрывного роста больших данных (Big Data). Исследуется «парадокс тёмной цифры», суть которого заключается в том, что несмотря на беспрецедентный рост объема и разнообразия цифровых следов, а также развитие технологий анализа информации, проблема неучтенной, скрытой преступности не только не решена, но и приобрела новые, более сложные формы.

Ключевые слова: Латентная преступность, тёмная цифра, Big Data, большие данные, методология криминологических исследований, киберпреступность, виктимизационный опрос.

Понятие «тёмной цифры» (dark figure) или латентной преступности является одним из фундаментальных и одновременно наиболее проблемных в криминологической науке. Оно отражает разрыв между преступностью реальной, совершаемой в обществе, и преступностью зарегистрированной, отраженной в официальной полицейской статистике. Борьба с этим разрывом, попытки измерить и объяснить природу латентности на протяжении десятилетий определяли развитие методологии социальных исследований, породив такие инструменты, как опросы потерпевших (виктимизации) и самоотчетов правонарушителей. Однако наступление эпохи Big Data – характеризующейся экспоненциальным ростом объема, скорости генерации и разнообразия цифровой информации, – поставило перед криминологией новые, парадоксальные вызовы.

С одной стороны, цифровая среда порождает иллюзию тотальной прозрачности. Социальные сети, электронные транзакции, данные сенсоров, коммуникационные метаданные создают невиданный ранее массив цифровых следов человеческой активности, включая противоправную. Кажется, что преступность, особенно в киберпространстве, должна быть как никогда видимой для анализа. С другой стороны, на практике мы наблюдаем обратное: новые формы преступности (крипто-мошенничества, фишинг, атаки на Интернет вещей, преступления в даркнете) обладают чрезвычайно высоким уровнем латентности. Традиционные методы измерения «тёмной цифры» оказываются малоэффективными, а попытки применить технологии Big Data наталкиваются на сложнейшие методологические, технические и этические барьеры. Таким образом, возникает «парадокс тёмной цифры» в эпоху Big Data: обладая беспрецедентными техническими возможностями для наблюдения и анализа, общество сталкивается с новой, более изощренной и скрытой преступностью, измерить масштабы которой становится все сложнее.

Традиционно криминология опиралась на три основных источника данных о преступности, каждый из которых пытался компенсировать недостатки другого: официальную статистику правоохранительных органов, выборочные опросы населения (виктимизационные исследования) и опросы самоотчетов. Виктимизационные опросы, ставшие золотым стандартом с середины XX века, позволили выявить огромный массив преступлений, не

ставших известными полиции, – от мелких краж до бытового насилия. Их сила заключалась в прямой репрезентации опыта жертв. Однако в цифровую эпоху эти методы сталкиваются с растущими проблемами.

Во-первых, возникает проблема репрезентативности и идентификации жертвы. Многие современные киберпреступления, такие как массовая утечка персональных данных, ботнет-атаки или майнинг-злоупотребления, не имеют конкретной, легко идентифицируемой жертвы в классическом понимании. Жертвой может быть миллион пользователей, чьи данные были скомпрометированы, причем они сами могут долгое время не знать об этом. Как справедливо отмечает криминолог Майкл Макгуайр, «киберпространство создает условия для “преступлений без жертв” в новом смысле – где вред диффузен, распределен и часто невидим для самого пострадавшего». Провести репрезентативный опрос среди таких рассредоточенных и неосведомленных жертв методически крайне сложно.

Во-вторых, семантический барьер между опытом пользователя и криминологической квалификацией события становится выше. Жертва фишингового письма может не считать себя жертвой преступления, а лишь собственной невнимательности. Пользователь, сталкивающийся с кибербуллингом или троллингом, может интерпретировать это как личный конфликт, а не как правонарушение. Вопросы в традиционных анкетах виктимизации часто не способны адекватно «уловить» эти новые формы виктимизации.

В-третьих, сама техника проведения опросов устаревает. Низкий уровень ответов на телефонные опросы, смещение выборки в сторону пожилых и менее «цифровых» слоев населения приводят к тому, что наиболее активная в цифровой среде и потому более виктимизированная молодежь оказывается недопредставленной в исследованиях. Таким образом, классические методы, направленные на освещение «тёмной цифры», сами погружаются в методологическую тень, будучи не в состоянии адекватно отобразить реалии цифровой преступности.

Парадокс заключается в кажущемся противоречии: инструментарий для сбора данных колоссально вырос, а прозрачность преступности – нет. Чтобы понять это, необходимо отказаться от наивного технологического детерминизма и рассмотреть природу как big data, так и современной латентной преступности.

1. Гносеологическая природа Big Data: следы и события. Big Data по своей сути – это совокупность цифровых следов, пассивно генерируемых в процессе взаимодействия человека с технологиями. Это данные о запросах, местоположении, транзакциях, социальных связях. Однако преступление – это событие, обладающее конкретной правовой квалификацией, умыслом, причинно-следственными связями. Между следом и событием лежит пропасть интерпретации. Миллиарды точек данных сами по себе не говорят о преступлении. Они могут содержать аномалии, паттерны, корреляции, но для их криминологической интерпретации необходима теория, гипотеза и контекст. Как отмечает Кейт Хорст, исследователь в области data science, «большие данные отвечают на вопрос “что”, но почти никогда – на вопрос “почему”». Обнаружив аномальный трафик с устройства, мы не знаем, является ли это признаком взлома, сбоя программного обеспечения или активности легитимного пентестера. Big Data создает «шум» невероятной громкости, в котором сигнал о реальном преступлении тонет.

2. Структурная латентность киберпреступности. Новые формы преступлений изначально спроектированы с высокой степенью латентности. Использование шифрования, анонимных сетей, криптовалют, стеганографии, одноразовых серверов делает цифровые следы фрагментированными, псевдонимизированными и трудносвязуемыми. Преступность мигрирует в даркнет – целенаправленно скрытую часть интернета, доступ к которой и сбор данных с которой представляют собой отдельную сложнейшую задачу. Таким образом, самая

опасная часть «тёмной цифры» целенаправленно укрывается в тех цифровых пространствах, где сбор Big Data либо технически невозможен, либо юридически запрещен.

3. Проблема «цифрового разрыва» в данных. Big Data страдает от систематических смещений (bias). Активность в социальных сетях, данные смартфонов, банковские транзакции – это данные в первую очередь об определенных социально-демографических группах (более молодых, обеспеченных, урбанизированных). Маргинализированные группы, пожилые люди, жители территорий с низким покрытием связью могут быть слабо представлены в этих массивах. Следовательно, и преступность, жертвами или субъектами которой они являются, также останется латентной для анализа, основанного на коммерческих или открытых Big Data. Мы рискуем получить искаженную картину, где гипервидимость одних видов преступности (например, кибермошенничества против среднего класса) соседствует с полной невидимостью других (например, цифровой эксплуатации уязвимых групп на закрытых форумах).

4. Этико-правовые ограничения и «слепые зоны». Тотальный мониторинг цифровых следов с целью выявления преступности входит в прямое противоречие с правами человека на приватность, защиту персональных данных и свободу коммуникации. Регламенты GDPR в Европе, аналогичные законы в других странах устанавливают жесткие рамки для сбора и обработки данных. Это создает законные «слепые зоны», куда исследователи и правоохранители не могут заглянуть без санкции. Таким образом, часть «тёмной цифры» остается латентной не по техническим, а по правовым причинам, что является принципиально новым вызовом для методологии. «Парадокс современной безопасности, – пишет философ технологии Зигмунт Бауман, – заключается в том, что стремление к абсолютной прозрачности граждан подрывает саму основу доверия, на которой зиждется общество».

Преодоление «парадокса тёмной цифры» требует не отказа от Big Data, а развития новой, гибридной методологической парадигмы, которую можно предварительно назвать криминологией данных. Ее суть – не в замене, а в синергии классических криминологических теорий и методов с передовыми технологиями анализа данных.

«Парадокс тёмной цифры» в эпоху Big Data является ярким проявлением более общего кризиса методологии социальных наук в условиях цифровой трансформации. Он демонстрирует, что технологический инструментарий, сколь бы мощным он ни был, не может автоматически решить концептуальные и гносеологические проблемы измерения сложных социальных феноменов, таких как преступность. Big Data, при всей их кажущейся всеохватности, оказываются страдающими собственными формами «латенции» – смещениями, шумом, семантическими разрывами и этическими «слепыми зонами».

Классические методы измерения латентной преступности, основанные на субъективном опыте и рефлексии жертв и правонарушителей, не утратили своей ценности, но требуют глубокой модернизации для учета реалий цифровой виктимизации. Проблема заключается не в выборе между «старыми» и «новыми» методами, а в поиске путей их интеграции.

Список литературы:

1. Дюркгейм, Э. Метод социологии / Э. Дюркгейм. – М.: Наука, 1991. – 572 с.
2. Биддерман, А.Д., Рейсс, А.Дж. Тёмные цифры преступности: вызов для социальных индикаторов // Социальные индикаторы. – 1967. – С. 127–142.
3. Майер-Шёнбергер, В., Кьюкьер, К. Big Data. Революция, которая изменит то, как мы живем, работаем и мыслим / В. Майер-Шёнбергер, К. Кьюкьер. – М.: Манн, Иванов и Фербер, 2014. – 240 с.
4. Макгуайр, М. Киберпреступность и кибербезопасность / М. Макгуайр. – М.: Когито-Центр, 2022. – 480 с.

5. Бауман, З., Лион, Д. Текучая слежка: разговор о слежке в современном мире / З. Бауман, Д. Лион. – М.: Ад Маргинем Пресс, 2019. – 168 с.
6. Гилинский, Я.И. Криминология: курс лекций / Я.И. Гилинский. – СПб.: Питер, 2024. – 512 с.