Научная статья
УДК 34:004:343.721:004.8
EDN: https://elibrary.ru/tnqlxy
DOI: https://doi.org/10.21202/jdtl.2025.21

Влияние киберпреступности на электронную коммерцию в Камеруне: социально-правовые и экономические последствия

Анумбуандем Бенволио Лекунзе

Университет Буэа, Буэа, Камерун

Ключевые слова

безопасность,
Камерун,
киберпреступность,
мошенничество,
право,
правосудие,
транзакции,
фишинг,
цифровые технологии,
электронная коммерция

Аннотация

Цель: проанализировать влияние киберпреступности на операции электронной коммерции в Камеруне и оценить эффективность существующих правовых механизмов противодействия киберугрозам.

Методы: исследование базируется на теориях утилитаризма, транзакционных издержек и рационального выбора. Применена методология качественного исследования с использованием доктринального метода. Проведен комплексный анализ правовых актов Камеруна в сфере кибербезопасности и электронной коммерции. Выполнено социологическое обследование с получением 250 выборочных ответов от жителей района Молико в городе Буэа в период с января по апрель 2025 г. Исследованы судебные прецеденты и статистические данные Министерства почты и телекоммуникаций Камеруна.

Результаты: установлено, что киберпреступления привели к потере доверия к операциям электронной коммерции в Камеруне, что отражается на снижении желания граждан осуществлять онлайн-транзакции. Выявлено, что более 60 % молодежи в возрасте от 16 до 35 лет в крупных городах Камеруна либо вовлечены в киберпреступления, связанные с электронной коммерцией, либо пострадали от них. Зафиксирован рост числа женщин среди киберпреступников. Определены основные виды киберпреступлений: мошенничество, фишинг и хищение средств с банковских карт.

Научная новизна: комплексный междисциплинарный анализ влияния киберпреступности на электронную коммерцию в контексте развивающейся африканской экономики. Впервые проведено эмпирическое исследование масштабов киберпреступности в конкретном регионе Камеруна с количественной оценкой вовлеченности молодежи в противоправную деятельность. Разработана теоретическая модель, объединяющая концепции утилитаризма, транзакционных издержек и рационального выбора для объяснения мотивации

киберпреступников. Выявлены специфические социально-правовые факторы, способствующие росту киберпреступности в условиях социально-политического кризиса.

Практическая значимость: результаты исследования имеют важное прикладное значение для совершенствования правовых, технологических, социальных и экономических механизмов противодействия киберпреступности в Камеруне. Предложенные рекомендации включают реформирование процессуального законодательства, расширение полномочий специализированных органов, введение системы домашних адресов и номеров социального страхования, повышение минимальной заработной платы и интеграцию курсов кибербезопасности в образовательные программы. Полученные данные могут быть использованы правительственными структурами, судебной системой, образовательными учреждениями и международными организациями для разработки эффективных стратегий борьбы с киберпреступностью и развития безопасной цифровой экономики.

Для цитирования

Лекунзе, А. Б. (2025). Влияние киберпреступности на электронную коммерцию в Камеруне: социально-правовые и экономические последствия. *Journal of Digital Technologies and Law*, *3*(3), 512–536. https://doi.org/10.21202/jdtl.2025.21

Содержание

Введение

Преступления – частое явление в каждом человеческом обществе, они появились в древности и продолжают существовать до сих пор (Chris et al., 2005). После того как 1 января 1983 г.[1] был открыт публичный доступ в Интернет, стало возможным совершение преступлений с помощью коммуникационных порталов в Сети, что изначально не было предусмотрено законодателем. Первое в истории зафиксированное киберпреступление произошло в 1834 г., когда была взломана система телеграфа во Франции и с помощью украденных данных был получен доступ к финансовым рынкам[2]. В отличие от обычных преступлений акт совершения киберпреступления включает в себя различные элементы, инструменты и процессы, вызывающие проблемы с юрисдикцией и доказыванием. Это объясняется тем, что киберпространство обширно и не ограничено географическим регионом или страной (Yokotani & Takano, 2021; 2022).

Киберпреступность можно определить как широкий спектр преступных действий, которые осуществляются с использованием цифровых устройств и сетей (Alhadidi et al., 2024; Arroyabe et al., 2024; Edwards & Hollely, 2023; Gupta et al., 2025; Higgs & Flowerday, 2025a)[3], а также как совокупность преступных действий, которые включают преступления против компьютеров и компьютерных систем (Payne, 2020). Компьютер может быть объектом совершения преступления или мишенью. Киберпреступностью также может называться любая преступная деятельность, в ходе которой компьютер используется как инструмент или средство совершения иных преступлений, например, в форме киберкражи или других связанных с ней незаконных действий, направленных против личности и собственности (Garner, 1999). Данная статья посвящена влиянию киберпреступлений на операции электронной коммерции (e-commerce) в Камеруне, поскольку научных исследований о влиянии киберпреступлений на коммерцию в Камеруне недостаточно. Примеры киберпреступлений включают, в частности, хакерские атаки, киберпреследование, диффамацию, бомбардировку электронными письмами, подделку данных, салями-атаки [также «салями-слайсинг» – метод киберпреступления, при котором злоумышленник совершает серию незначительных действий или краж, которые в совокупности могут привести к серьезному ущербу или компрометации данных, ресурсов или активов. – Прим. переводчика], отказы в обслуживании, атаки вирусов и червей, кражи интернет-времени и т. д. Операции электронной коммерции, как следует из названия, осуществляются в киберпространстве посредством однорангового электронного обмена данными (electronic data interchange, EDI) (Garner, 1999) и могут сопровождаться преступлениями.

---

1 1 января 1983 г. считается официальным днем рождения Интернета. До этого различные компьютерные сети не имели стандартного способа взаимодействия друг с другом. Был разработан новый протокол связи под названием Протокол межсетевого взаимодействия (Transfer Control Protocol/ Internetwork Protocol, TCP/IP). Это позволило осуществить коммуникацию между различными типами компьютеров в разных сетях. 1 января 1983 г. ARPANET и сеть передачи данных Министерства обороны официально перешли на стандарт TCP/IP, что стало рождением Интернета. https://clck.ru/3QEh9u

2 Blue Voyant. https://clck.ru/3QEh97

3 Следует отметить, что киберпреступления чаще совершаются в сфере коммерческих операций, чем в других областях.

Электронная торговля может принимать формы онлайн-покупок, общения с мобильными приложениями посредством чатов, чат-ботов и голосовых помощников[4]. Выделяют такие типы взаимодействия, как «бизнес-бизнес» (B2B), «бизнес-клиент» (B2C), «клиент-клиент» (C2C) и «клиент-бизнес» (C2B). Это практика покупки и продажи товаров и услуг через онлайн-сервисы для потребителей в Интернете и один из способов ведения бизнеса компаниями и частными лицами с целью максимизации прибыли в короткие сроки при одновременном снижении как постоянных затрат на широкий спектр активов, так и транспортных расходов из центральных деловых районов[5].

Электронная торговля обладает рядом преимуществ, однако киберпреступления препятствуют бесперебойному функционированию электронной коммерции и приводят к потере прибыли и доверия деловых партнеров. В Камеруне предпринимаются усилия по борьбе с киберпреступлениями с помощью законодательства и технологий, но пока они не оказали существенного влияния на коммерческие операции из-за недостатка новых технологий, слабой системы управления цифровыми правами[6], а также из-за простоты обхода технологических мер, удобства и скорости совершения киберпреступлений. Кроме того, преступники получают выгоды и удовлетворение, обходя те самые технологии, которые предназначены для защиты от киберпреступлений в рамках операций электронной коммерции.

В последние годы в Камеруне наблюдается рост числа киберпреступлений и связанных с ними правонарушений в сфере коммерческих операций в связи с расширением распространения Интернета, низкой стоимостью приобретения электронных устройств, глобальным экономическим кризисом, карантином из-за пандемии COVID-19 и появлением многочисленных платформ социальных сетей. Киберпреступления стали популярны в Камеруне примерно в 2005 г., до вступления в силу в 2010 г. законов о киберпреступности и электронной торговле. Это можно продемонстрировать на примере более ранних судебных дел: The People v. Obi Roland[7], The People v. Nfang Macknight[8], The People v. Mbah Valery[9], The people of Cameroon v. Tamukum Fonjiyang Ferdinand & one other[10], The people of Cameroon & another v. Tita Njina Kevin Ndango[11]. Все они рассматривались до принятия в 2010 г. законов о киберпреступности и электронной торговле в Камеруне, хотя о некоторых

4 VentureBeat. (2025, March 15). How to prepare your products and brand for conversational commerce. https://clck.ru/3QEhWE

5 Это положение объясняет теория сельского хозяйства фон Тюнена, разработанная Иоганном Генрихом фон Тюненом в 1826 г. Эта модель предсказывает поведение человека с точки зрения ландшафта и экономики на основе тщательных математических расчетов и наблюдений. Она объясняет стоимость транспортировки от географического расположения фермы до центрального делового района города. Разработанная для сельского хозяйства, сегодня эта теория относится к электронной коммерции, поскольку основной целью электронной коммерции является минимизация транзакционных издержек от места происхождения товаров и услуг до места нахождения потребителя.

6 Речь идет о технических способах защиты данных с использованием паролей, криптографии и стеганографии.

7 CFIB/55C/2008(Unreported).

8 CFIB/76C/2009(Unreported).

9 CFIB/255/2010(Unreported).

10 (2014) 2 SLR.

11 (2010) CCLR 1-126

из этих дел стало известно позже. При этом можно заметить, что гражданские стороны этих процессов практически не присутствовали в суде, что вызвало всплеск киберпреступлений в Камеруне. Этот аспект мы затронем ниже в данной работе.

Первые законодательные акты о киберпреступлениях и электронной торговле в Камеруне были приняты в декабре 2010 г. после участившихся случаев киберпреступности в стране. Они в основном касались коммерческих операций с использованием онлайн-платформ, которые представляли собой мошенничество[12] под видом законных деловых операций[13]. Именно поэтому Закон о киберпреступности и Закон об электронной торговле в Камеруне были приняты в одном и том же году.

В данной статье рассматривается влияние киберпреступности на операции электронной коммерции в Камеруне. Наряду с Уголовным и Уголовно-процессуальным кодексами Камеруна правовую основу для расследования и судебного преследования за киберпреступления обеспечивает Закон о киберпреступности. Он предусматривает различные виды киберпреступлений, включая незаконный перехват данных, хакерские атаки, компьютерное мошенничество, преступления, связанные с детской порнографией, и т. д. Этот закон носит не только адъективный, но и процедурный характер, поскольку он устанавливает правила расследования и судебного преследования киберпреступлений в условиях международного сотрудничества.

С другой стороны, основы электронной торговли в Камеруне заложил Закон об электронной торговле от 2010 г.[14] Это произошло из-за стремительного развития платформ электронной коммерции в русле мировых тенденций. Закон также предусматривает все существенные элементы и процедуры для расследования и судебного преследования по искам о нарушениях в рамках электронных сделок.

Киберпреступления в Камеруне связаны не только с операциями электронной коммерции, но и с другими преступными деяниями, такими как диффамация, мошенничество, кражи, киберпреследование и хакерские атаки. Закон № 2010/012 от 21 декабря 2010 г. о кибербезопасности и киберпреступности в Камеруне предусматривает уголовную ответственность за киберпреступления, как и Закон № 2016/007 от 12 июля 2016 г. в Уголовном кодексе[15]. Закон № 2010/021 от 21 декабря 2010 г. об электронной торговле в Камеруне устанавливает правонарушения и наказания за нарушение положений правил электронной торговли. Влияние киберпреступности на электронную коммерцию в Камеруне огромно, учитывая тот факт, что большинство граждан страны не владеют компьютерной грамотностью и не могут позволить себе подключение к Интернету для изучения деятельности на электронных коммерческих площадках. Это приводит к ряду юридических

12 Закон № 2016/007 от 12.08.2016. Раздел 318.

13 Киберпреступность в Камеруне была официально признана как юридическая проблема в декабре 2010 г. с принятием Закона № 2010/012, который определяет киберпреступления и предусматривает наказание за них. До принятия этого закона многие случаи киберпреступности рассматривались в соответствии с Уголовным кодексом Камеруна.

14 Закон № 2010/021 от 21.12.2010.

15 Уголовный кодекс Камеруна. Раздел 219.

проблем, таких как злоупотребление доверием, потеря прибыли как на микро-, так и на макроэкономическом уровнях, рост взяточничества и коррупции и общий рост преступности, поскольку незаконные доходы, полученные в результате таких преступных деяний, часто используются для совершения новых преступлений.

1. Постановка проблемы

Внедрение электронной коммерции в Камеруне и распространение киберпреступности имели разрушительные последствия для бизнеса, основанного на цифровых технологиях. Ситуация усугубляется тем, что подавляющее большинство населения Камеруна получает зарплату ниже уровня минимальной заработной платы, а также в стране отсутствует система официальных домашних адресов и номеров социального страхования граждан. Отсутствие цифровых домашних адресов и номеров социального страхования затрудняет проведение расследований, выдачу повесток и арестов, поскольку доставка[16] обычно осуществляется в почтовых отделениях или в других местах по требованию, а платежи переводятся на банковские счета, которые не привязаны к конкретным адресам их владельцев. В настоящее время в Камеруне все чаще наблюдается потеря доверия к электронным коммерческим операциям, поскольку многие платежи являются необеспеченными[17]. Это приводит к огромным потерям прибыли и росту преступности по всей стране, поскольку незаконные доходы, полученные от киберпреступлений, часто используются для содействия совершению других преступлений, таких как злоупотребление наркотиками, взяточничество, коррупция, преступления против нравственности, пьянство в общественных местах и т. д. Киберпреступления также привели к широкому распространению произвольных, без наличия весомых доказательств, арестов и пыток, особенно в отношении молодежи, поскольку некоторые сотрудники полиции и судебных органов принимают на веру обвинения в мошенничестве из-за образа жизни даже без каких-либо официальных исков. Большинство из этих сотрудников практически не занимаются расследованием киберпреступлений в сфере электронной коммерции, а предпочитают обогащаться, получая взятки за освобождение подозреваемых. Это усугубляется тем фактом, что большинство жертв не подают официальных жалоб на преступников. В Камеруне также наблюдается низкий уровень международного сотрудничества в борьбе с киберпреступлениями, связанными с электронной коммерцией, из-за неадекватной технической инфраструктуры, личной финансовой выгоды и отсутствия надлежащего контроля. Это привело к росту числа таких киберпреступлений в стране, причем большинство правонарушителей предпочитают давать взятки и находят других жертв, чтобы возместить свои убытки[18]. Кроме того, существует общая атмосфера боязни подавать официальные жалобы на киберпреступников из-за позора и возможных тяжелых последствий, поскольку большинство

[16] Хотя для задержания подозреваемых в почтовых отделениях могут осуществляться контролируемые доставки, в Камеруне это почти не практикуется.

[17] Правила возврата денег в Камеруне крайне неэффективны и практически не закреплены в коммерческих контрактах. Таким образом, у клиентов возникают опасения.

[18] Можно заметить, что большинство киберпреступников в сфере электронной коммерции не прекращают свои действия даже после того, как обогатились. В основном они совершенствуют свои навыки.

жертв с самого начала являются сообщниками преступников в совершении незаконных операций. Все эти проблемы усугубились из-за отсутствия достаточных полномочий у таких ведомств, как Национальное агентство финансовых расследований (National Financial investigation agency, NFIA) и Национальное агентство информационно-коммуникационных технологий (National Agency for information and communication technologies, NAICT), для судебного преследования киберпреступлений в Камеруне. Их функции сводятся к подаче исков, проведению расследований и вынесению рекомендаций без надлежащего контроля.

2. Теоретические и концептуальные основы

Настоящее исследование базируется на ряде теоретических положений.

2.1. Теория утилитаризма

Данная теория была выдвинута Джоном Стюартом Миллем в 1861 г. Он считал, что счастье – это единственное, чего люди могут и должны желать ради самих себя. Теория гласит, что поскольку счастье – это единственное внутреннее благо и большее счастье предпочтительнее меньшего, то цель этической жизни – максимизировать счастье. Джереми Бентам и Джон Стюарт Милль назвали это положение «принципом полезности», или «принципом наибольшего счастья». В контексте нашего исследования киберпреступления в сфере электронной коммерции удовлетворяют потребности, обеспечивают благополучие и счастье преступников. Таким образом, стремление правонарушителей удовлетворить свое личное эго и обрести счастье побуждает их желать выгоды от обмана других людей путем совершения киберпреступлений в рамках электронной коммерции для получения удовольствия и удовлетворенности. Эта теория согласуется с теорией ресурсоемкой оценочно-максимизирующей модели (Resourceful Evaluative Maximizing Model theory), которая рассматривает индивидов как рациональных субъектов, всегда стремящихся максимизировать для себя пользу или благополучие в рамках заданного набора ограничений. Это показывает, что люди всегда стремятся найти наилучший возможный результат с учетом ограниченности своих ресурсов (Wartiovaara, 2011).

2.2. Теория транзакционных издержек

Эта теория была предложена Джоном Р. Коммонсом в 1931 г. (Williamson, 2008). Речь идет об издержках, возникающих в ходе торговли. Эти издержки связаны с управлением экономической системой компании и общими затратами на проведение транзакции. Сюда также входят затраты на планирование, принятие решений, изменение планов, разрешение споров и послепродажное обслуживание. По мнению автора теории, детерминантами операционных издержек являются частота, специфичность, неопределенность, ограниченная рациональность и оппортунистическое поведение. Одной из целей электронной коммерции является существенное снижение транзакционных издержек посредством электронного обмена данными (electronic data interchange, EDI). Теория транзакционных издержек (Transaction Cost Theory, TCT) изучает минимальные объемы ресурсов и затраты, необходимые сторонам для обмена товарами и услугами. Цель этой теории – максимизировать эффективность транзакций при минимизации затрат, что также является основной целью электронной

коммерции. Эту теорию можно сравнить с моделью фон Тунена, которая рассматривает транзакционные издержки, такие как перевозка урожая с ферм в центральный деловой район города. Цена продажи в основном определяется в зависимости от расстояния между центральным деловым районом и местом продажи сельскохозяйственной продукции. Эта теория связана с электронной коммерцией тем, что фокусируется на расстоянии между местами, где расположены товары и услуги, где проводятся переговоры о закупках и куда доставляются товары. Электронная коммерция в соответствии с этой моделью приводит к снижению затрат, независимо от того, где производятся товары и куда они доставляются, в отличие от обычных сделок, при которых сторонам приходится преодолевать большие расстояния для проведения переговоров и совершения покупок в реальном мире.

2.3. Теория рационального выбора

Эта теория была выдвинута Адамом Смитом в 1776 г. и позже сформулирована социологом Джорджем Хомансом в 1961 г. Она основана на поведенческой психологии и предполагает достижение цели с использованием наиболее экономичного метода, независимо от ценности этой цели. Цели могут быть корыстными, эгоистичными или материалистическими (Snidal, 2013). Теория дает рекомендации, которые помогают понять экономическое и социальное поведение и используются в криминологии. Это позволяет предсказать характер и результат выбора. Предполагается, что люди руководствуются личными интересами, а их решения основаны на оптимизации предпочтений путем балансирования затрат и выгод. Это явление распространено в электронной коммерции, где доступно множество вариантов онлайн-покупок и можно сделать свой выбор. Цели киберпреступников в сфере электронной коммерции обычно сосредоточены на них самих; они не заботятся о вреде, который причиняют своим жертвам, лишая их денежных средств. Эта теория также применима к случаям, когда человек принимает решение пойти на риск, чтобы совершить преступление и остаться на свободе, при этом получив выгоду. Это типичное явление в киберпреступлениях, связанных с электронной коммерцией, когда трудно поймать преступников на месте преступления.

3. Обзор научной литературы

Ряд авторов изучали области киберпреступности и электронной коммерции, не придавая особого значения связи между ними. Хотя некоторые авторы обращали внимание на влияние киберпреступности на операции электронной коммерции, они не исследовали критически взаимосвязь между ними, которая носит метафорический характер. Это объясняется тем, что те же санкции, которые применяются к обычным преступлениям в рамках коммерческих операций, применяются и к киберпреступлениям в рамках операций электронной коммерции. То, что происходит в реальном мире, ничем не отличается от того, что происходит в режиме онлайн, с той разницей, что в последнем случае для выполнения одного и того же действия используются определенные настройки и интерфейсы.

Reyns и соавторы (2011) подробно изучали опасения, вызываемые киберпреступлениями из-за виктимизации. Авторы исследуют взаимосвязь между риском в киберпространстве и страхом стать жертвой киберпреступности. Их анализ основан на информации, полученной от студентов Университета Цинциннати. Исследование

показало, что многие люди опасаются стать жертвами киберпреступлений. Авторы также выделяют категории правонарушителей и их поведенческие особенности в зависимости от статуса и пола. В работе рассматриваются особенности поведения, которые оказывают существенное влияние на уровень страха перед киберпреступностью. Авторы показывают, что страх и виктимизация в киберпространстве основаны на предполагаемых рисках. В работе не анализируются способы ослабить эти страхи, чтобы стимулировать электронную коммерцию.

Böhme и Moore (2012) описали киберпреступления в сфере онлайн-покупок и способы их предотвращения. Их основной вывод состоял в том, что киберпреступления приводят к снижению количества транзакций, таких как онлайн-банкинг и покупки онлайн, что имеет огромные негативные последствия. В работе показано, что люди, которые не знают о киберпреступлениях, с большей вероятностью совершают транзакции в рамках электронной коммерции, например, покупки онлайн. Исследование в основном посвящено онлайн-покупкам, в то время как понятие электронной коммерции гораздо шире.

В работе Y. Abubakari (2020) показано, что люди упускают множество возможностей из-за страха быть обманутыми. Автор пишет о причинах, последствиях и ограничениях политики в области киберпреступности в англоязычной Западной Африке. Он также демонстрирует, что киберпреступники теряют интерес к получению образования и что причина роста киберпреступлений связана с экономической напряженностью и коррупцией на правительственном уровне. Автор рассматривает препятствия в борьбе с киберпреступностью, такие как коррупция, вмешательство правительства, неэффективное применение законов о борьбе с киберпреступностью и непоследовательность соответствующих мер. Исследование фокусируется на Гане, Нигерии и странах Африки к югу от Сахары в качестве репрезентативной выборки для англоязычной Западной Африки, поскольку распространенность интернет-мошенничества в Западной Африке особенно высока в таких англоязычных странах, как Гана, Нигерия, Либерия, Сьерра-Леоне, Гамбия и часть Камеруна, достигает наибольших масштабов в Нигерии и Гане.

Исследование авторов Boraine и Leno Doris (2019) посвящено борьбе с киберпреступностью в Камеруне. Они сосредоточились главным образом на конфликте в англоязычных регионах страны и показали связь между этим конфликтом и ростом числа киберпреступлений. Были также проанализированы роль правительства Камеруна в борьбе с киберпреступлениями и некоторые правовые положения, используемые для борьбы с киберпреступлениями в стране. В работе рассматривались причины распространенности киберпреступлений и рекомендовались меры, которые могут быть приняты для борьбы с ними. Авторы не показали прямого влияния киберпреступлений на операции электронной коммерции. Исследование способствует углублению знаний о правилах защиты данных, особенно среди сотрудников следственных органов, студентов, специалистов и юристов-практиков.

Большая часть доступной литературы, рассмотренной выше, посвящена либо киберпреступности, либо электронной коммерции. В настоящей статье мы покажем непосредственное влияние киберпреступлений на операции электронной коммерции в Камеруне и дадим рекомендации по решению данной проблемы.

4. Распространенные типы киберпреступлений в сфере электронной коммерции в Камеруне

Киберпреступления в сфере электронной коммерции в Камеруне привели к потере примерно 12,2 млрд франков CFA в 2021 г., причем примерно половина этой суммы приходится на мошенничество и фишинг[19]. Существуют различные виды киберпреступлений, связанных с электронной коммерцией, которые затрагивают Камерун и весь мир. Очевидно, что характер коммуникаций в киберпространстве не ограничивает киберпреступления определенными географическими территориями. Человек может находиться в одной стране и совершать киберпреступления в разных странах с разными правовыми системами. Таким образом, существует необходимость в международном сотрудничестве для борьбы с киберпреступлениями, особенно с киберпреступлениями, связанными с электронной торговлей. По этой же причине истцы не обращаются в судебные инстанции, а число киберпреступлений растет[20]. Виды киберпреступлений, связанных с электронной коммерцией, включают, в частности: рассылку спама, салями-атаки, распространение вирусов, кибердиффамацию и т. д. Распространенными видами киберпреступлений в Камеруне являются мошенничество[21], фишинг[22] и хищения с банковских карт[23]. Большинство этих преступлений направлены на получение финансовой выгоды и совершаются в сфере электронной коммерции между отдельными гражданами.

4.1. Мошенничество

Мошенничество (scamming) – это получение денег или каких-либо преимуществ нечестным путем, особенно путем обмана. Такой обман может принимать большие масштабы. Мошенничество в Камеруне встречается относительно редко[24]. Этот термин также означает уловку, направленную на то, чтобы обмануть человека или группу людей, завоевать их доверие, воспользовавшись такими факторами, как наивность, сострадание, тщеславие, самоуверенность или жадность жертвы (Orbach & Huang, 2018). Согласно отчету Министерства почты и телекоммуникаций за 2021 г., уровень мошенничества в Камеруне составил 60 % в городах Яунде, Дуала, Буэа и Нун среди безработной молодежи в возрасте от 16 до 35 лет[25].

---

19 Отчет Министерства почты и телекоммуникаций Камеруна за 2021 г. Прим. 30. https://clck.ru/3QMjCH

20 Одной из причин нежелания преследовать киберпреступников в судебном порядке в Камеруне является то, что пострадавшие иногда являются гражданами других стран и их судебное преследование затруднено из-за ряда юридических сложностей, затрат и опасений. Это приводит к взяточничеству и коррупции, поскольку пострадавшие могут находиться в другой стране.

21 Обман с использованием протоколов электронной связи.

22 Преступник выдает себя за доверенное лицо, чтобы получить доступ к конфиденциальной информации.

23 Преступник получает данные банковской карты, когда ее владелец пользуется банкоматом.

24 Отчет Министерства почты и телекоммуникаций Камеруна за 2021 г. Прим. 6, с. 1346. https://clck.ru/3QMjCH

25 Там же.

Мошенничество – не новое явление, но оно усилилось с распространением ИКТ и Интернета. Еще в Древней Греции существовали наперсточники. Также в Греции «мошенник на доверии» по имени Томпсон выманивал деньги и был арестован в июле 1849 г.[26] Киберпреступления, связанные с электронной коммерцией, распространились в Камеруне в 2005 г., до вступления в силу Закона о кибербезопасности 2010 г. До этого суды при рассмотрении таких дел в основном полагались на Уголовный кодекс[27], как в деле The People v. Obi Roland[28]. Это дело о мошенничестве рассматривалось судом первой инстанции города Буэа в 2008 г., еще до вступления в силу законов о кибербезопасности и электронной коммерции 2010 г. В основу приговора была положена статья 318 Уголовного кодекса Камеруна. Обвиняемый был признан виновным и приговорен к шести годам тюремного заключения. В деле The People v. Nfang Macknight[29] тот же суд признал обвиняемого виновным по аналогичным основаниям.

Хотя суды часто выносят обвинительные приговоры, многие из таких дел в Камеруне не доходят до суда. Процедура рассмотрения дел о кибератаках часто изобилует несоответствиями, такими как нарушение прав, предусмотренных ст. 3 и 8 УПК, что привело к освобождению некоторых обвиняемых, как в делах The People v. Mbah Valery[30] и The people of Cameroon v. Tamukum Fonjiyang Ferdinand & one other[31]. Можно заметить, что из-за высокого уровня взяточничества и коррупции в делах о киберпреступлениях, связанных с электронной коммерцией, таких как мошенничество, суды в Камеруне в настоящее время практически не рассматривают такие дела. Мошенники и следователи предпочитают вступать в сговор, давая и получая взятки в обмен на свободу. Однако это может оказаться затруднительным в ситуациях, когда истец решает продолжить судебное преследование, подав гражданский иск в соответствующий суд. Так было в деле The people of Cameroon & another v. Tita Njina Kevin Ndango (Jansson & von Solms, 2011), когда суд первой инстанции города Буэа признал обвиняемого виновным по всем пунктам обвинения, поскольку истец прибыл из Швейцарии для участия в слушании.

4.2. Фишинг

Это вид мошенничества, при котором жертв обманом заставляют раскрыть конфиденциальную информацию или устанавливают вредоносное ПО, которое совершает салями-атаки, содержит вирусы или программы-черви, которые отображают нужный веб-сайт (Jansson & von Solms, 2011). Например, в написание названия или адрес сайта вносятся небольшие изменения, чтобы он походил на оригинальный, так что жертва не подозревает, что имеет дело с поддельным веб-сайтом.

---

26 Отчет Министерства почты и телекоммуникаций Камеруна за 2021 г. Прим. 29. https://clck.ru/3QMjCH

27 Закон № 2016/007 от 12 июля 2016 г. в Уголовном кодексе Камеруна.

28 CFIB/55C/2008(Unreported).

29 CFIB/76C/2009(Unreported).

30 CFIB/255/2010(Unreported).

31 (2014) 2 SLR.

Фишинг широко используется в Камеруне в мобильных сетях, когда жертвам звонят или отправляют текстовые сообщения-приманки с мобильного телефона. Поддельные сообщения, как правило, ссылаются на ошибочные денежные переводы на мобильные счета жертв. Злоумышленник тем временем вводит номер телефона жертвы в компьютерное приложение оператора мобильной связи (APP). Затем злоумышленник обманом заставляет жертву подтвердить данные своей учетной записи мобильного телефона, введя свой пароль для возврата денег с обещанием вознаграждения. Если жертва запрашивает услугу «мобильные деньги» на свой счет и вводит свой пароль на своем устройстве, он одновременно передается в приложение злоумышленника, где тот получает доступ к снятию или переводу средств. Эта схема широко распространена в Камеруне, и почти все пользователи мобильных телефонов столкнулись с этим явлением, причем большинство попалось на уловку. Это не только порождает страх, но и создает искаженное представление об электронной коммерции, осуществляемой компаниями мобильной связи, как об одном из способов мошенничества. Некоторые дела такого рода успешно рассматривались в судах, поскольку можно было отследить номер злоумышленника, но иногда преступники проявляли достаточную сообразительность, регистрируя счета для снятия средств на имена разных физических лиц, которые находятся в разных географических точках.

4.3. Хищение средств с банковских карт

При этом способе хищения (skimming) на банкоматах или внутри них, а также в других точках продаж устанавливаются технологические устройства, с помощью которых злоумышленники могут записывать данные карты и копировать их[32]. Ту же тактику преступники используют для получения конфиденциальной информации с дебетовой или кредитной карты. Эти устройства собирают и хранят данные, которые мошенники впоследствии используют для совершения покупок или снятия средств в разное время[33]. Скимминг банковских карт не очень распространен в Камеруне из-за отсутствия необходимых технологических устройств, а также из-за того, что большинство банкоматов и точек продаж оснащены камерами видеонаблюдения и охраной. Однако скиммеры также могут физически украсть данные карты, если оставить ее в зоне доступа.

4.4. Социально-правовые последствия киберпреступности для электронной коммерции в Камеруне

Киберпреступность имеет множество негативных последствий для бизнеса и пользователей электронной коммерции, начиная от потери доверия и заканчивая банкротством предприятий и другими социальными проблемами в разных странах (Luu et al., 2025; Higgs & Flowerday, 2025b; Lee et al., 2023; Holt, 2022; Hornuf et al., 2025). Киберпреступления, связанные с электронной коммерцией, имеют социальные

32 Federal Bureau of Investigation. Skimming. https://clck.ru/3QEhzV

33 BrightBridge Credit Union. https://clck.ru/3QEi7p

и юридические последствия и порождают страх перед виктимизацией у потенциальных пользователей, готовых оплачивать товары и услуги через онлайн-платформы. Страх – это фактор, который влияет на физическое и психологическое состояние каждого человека. Это подрывает доверие и заставляет граждан задуматься о балансе издержек и выгод. В результате они отдают предпочтение наличным расчетам[34].

Распространение киберпреступлений в сфере электронной коммерции можно объяснить с точки зрения теорий утилитаризма и рационального выбора[35], согласно которым люди склонны занимать положение, обеспечивающее максимальное удовлетворение их потребностей, даже если это означает принятие иррациональных решений, которые иногда могут привести к достижению позитивной цели, не опасаясь последствий. Утилитаристская точка зрения рассматривает удовлетворение как фактор, который может перевесить рациональное поведение. Это объясняет, почему занимаются мошенничеством большинство молодых камерунцев в таких районах, как Молико и Бамбили, в городах Буэа и Баменда, соответственно. Киберпреступность в сфере электронной коммерции также быстро растет в англоязычных регионах Камеруна из-за текущего социально-политического конфликта. Эта ситуация еще более усугубляется высоким уровнем безработицы среди молодежи, низким уровнем минимальной заработной платы и общей шкалы оплаты труда в стране[36]. Многие молодые люди в этих районах Камеруна, особенно женщины, открывают поддельные интернет-магазины, якобы осуществляющие электронные коммерческие операции через платформы социальных сетей, чтобы скрыть незаконные источники своего дохода. В прошлом киберпреступления, связанные с электронной коммерцией, в основном совершались мужчинами, которые прибегали к обману, создавая в электронном виде редкие изображения несуществующих предметов и животных, чтобы привлечь внимание жертв.

Благодаря внедрению современной инфраструктуры ИКТ и легкому доступу к Интернету по доступным ценам в Камеруне мошенничество и фишинг в настоящее время распространены в большинстве густонаселенных городов. В период с января по апрель 2025 г. в районе Молико в Буэа автором был проведен опрос и получено 250 выборочных ответов от случайных участников. Было обнаружено, что по меньшей мере 60 % молодых людей в Молико вовлечены в киберпреступления, связанные с электронной коммерцией. Собранные данные также показали, что 10 % преступников – женщины, а 50 % – мужчины в возрасте от 16 до 35 лет. Также было отмечено, что большинство жертв проживали в Молико и преступники были знакомы со своими жертвами. Преступники не были знакомы лишь с несколькими жертвами, которые проживали в разных городах Камеруна и за рубежом.

Исследование также показало, что незаконные финансовые доходы, получаемые в результате этих киберпреступлений, значительно различаются по суммам: лишь немногие преступники зарабатывают огромные суммы почти регулярно, в то

---

34 Многие камерунцы предпочитают оплачивать товары наличными, чтобы их можно было увидеть и оценить. Именно по этой причине большинство жителей Камеруна пользуются наличными, несмотря на связанные с этим риски.

35 См. выше раздел «Теория рационального выбора».

36 Минимальная заработная плата в Камеруне на 46 939 франков CFA меньше, чем в соседних африканских странах.

время как некоторые едва зарабатывают на ежедневные карманные расходы. Деятельность злоумышленников в основном была связана с мошенничеством и фишингом. Опрос показал, что большинство молодых людей в Молико вовлекаются в эту деятельность из-за желания удовлетворить свое эго с помощью денег; другими мотивами являются конкуренция, давление со стороны сверстников, склад характера и незначительное число судебных преследований благодаря коррупции. Также был сделан вывод, что большинство преступников по-прежнему активно участвуют в киберпреступлениях в сфере электронной коммерции и при этом продолжают совершенствовать свои навыки.

Также было обнаружено, что многие молодые люди бросили школу, как отмечал Юшаву Абубакари в статье, опубликованной в 2020 г. (Abubakari, 2020).· При этом некоторые молодые люди, занимавшиеся киберпреступностью, платили другим из своих незаконных доходов за сдачу школьных экзаменов[37].

Оккультные практики[38] также широко распространены среди киберпреступников в Камеруне, что приводит к печальным последствиям, поскольку большинство молодых людей с низкими интеллектуальными способностями убеждены, что успех их незаконной деятельности зависит от таких практик. Это привело к нескольким смертельным случаям и появлению организованных банд мошенников, которые иногда совместно дают взятки, чтобы «выручить» своих коллег, попавших в беду. Оккультные практики распространяются и на другие социальные сферы, такие как гомосексуализм, лесбийские практики, инцест и другие сексуальные действия[39].

Все эти факторы, как отмечалось ранее, способствовали высокому уровню отсева из школ, тем самым повышая уровень неграмотности среди молодежи в Камеруне. В то же время правительство Камеруна, несмотря на это, продолжает вкладывать средства в образование молодежи, субсидируя начальное, среднее и высшее образование по всей стране.

4.5. Распространение иных типов преступлений в связи с киберпреступностью в сфере электронной коммерции

Незаконное обогащение в результате киберпреступлений в сфере электронной коммерции приводит к распространению других преступлений, таких как злоупотребление наркотиками, проституция, пьянство в общественных местах, выдача себя за другое лицо на экзаменах, сексуальные преступления, диффамация, насилие, коррупция, кража личных данных, нападение, нанесение побоев, неосторожное вождение и т. д. Неожиданное обогащение может привести к развитию психопатических наклонностей, особенно среди молодых людей, чья психика еще не сформирована. Это также было отмечено в ходе проведенного опроса.

---

37 Некоторые случаи выдачи себя за другое лицо были выявлены во время заседаний дисциплинарного совета руководством университетов, расположенных в Молико.

38 Оккультизм – это различные практики и верования, связанные с изучением манипулирования сверхъестественными силами. Эта сфера включает широкий спектр практик, включая гадание, магию, алхимию, астрологию и спиритизм.

39 Однако сегодня в Камеруне есть правозащитники, которые осуществляют деятельность, направленную на защиту прав лесбиянок, геев, бисексуалов, трансгендеров и квир-людей (ЛГБТК) (Международное общественное движение ЛГБТ признано экстремистским и запрещено на территории РФ).

4.5.1. Утрата доверия пользователей в сфере электронной коммерции

Сегодня в Камеруне часто можно увидеть молодых людей, которые ведут эпатажный образ жизни и ездят на автомобилях определенных марок, не имея никаких доказательств своих финансовых возможностей. Это напрямую связано с высоким уровнем киберпреступлений и коррупции в сфере электронной коммерции. Индекс коррупции в Камеруне, по данным организации Transparency international, в 2024 г. составил 26 пунктов из 100, что намного выше, чем в большинстве стран мира[40]. Это происходит, в частности, из-за киберпреступлений в сфере электронной коммерции и безответственного отношения к расследованию таких преступлений, что связано со взяточничеством и коррупцией в стране и не получает реакции на уровне Интерпола.

Закон о кибербезопасности 2010 г. устанавливает юрисдикцию и полномочия сотрудников следственных органов[41], которые должны соблюдать уголовно-процессуальные нормы, закрепленные в Уголовно-процессуальном кодексе 2005 г.[42] Но, к сожалению, большинство из этих сотрудников вступают в сговор с преступниками ради личной выгоды, и поэтому большинство дел о киберпреступлениях не доходят до надлежащего рассмотрения в суде[43]. Нередки случаи, когда сотрудники полиции и жандармерии арестовывают подозреваемого в киберпреступлении из-за его подозрительной финансовой деятельности даже без заявления, а затем сопровождают подозреваемого к банкоматам, чтобы забрать свою предполагаемую долю незаконно полученных денег. Такие полицейские заставляют подозреваемых переводить деньги с их мобильных счетов на их собственные телефоны, а затем отпускают. Часто можно увидеть, как сообщники подозреваемых дают взятки за освобождение одного из них, попавшего в беду. Некоторые киберпреступники включают в свой список сотрудников правоохранительных органов, которые защищают их от любых возможных неожиданностей. Подозреваемые, которые отказываются сотрудничать с полицией, чаще подвергаются необоснованным арестам и содержанию под стражей с применением пыток. В связи с этим возникает вопрос о надлежащей правовой процедуре и несоблюдении сотрудниками полиции нормы о запрете пыток, закрепленной в Международном пакте о гражданских и политических правах (МПГПП), Африканской хартии прав человека и народов (АХПЧН) и актах национального законодательства.

Все эти негативные аспекты в значительной степени подорвали доверие граждан страны как внутри страны, так и за рубежом. Из-за отсутствия доверия снижены возможности для осуществления законных операций в сфере электронной коммерции в Камеруне с иностранными гражданами. Можно отметить, что многие камерунцы, проживающие за рубежом, хорошо известны своими киберпреступлениями, а некоторые из них отбывают длительные тюремные сроки в зарубежных странах. Феномен сокрытия киберпреступлений за взятку наблюдается сегодня во многих африканских странах (Sarefo et al., 2023; Matias, 2025). Большинство сотрудников следственных органов предпочитают брать взятки, а не преследовать виновных в суде.

---

40 Transparency International. https://clck.ru/3QEjAB

41 Закон № 2010/012 от 21 декабря 2010 г. О кибербезопасности и киберпреступности в Камеруне. Раздел 52(1).

42 Закон № 2005 от 27 июля 2005 г. об Уголовном-процессуальном кодексе Камеруна. Разделы 59 и 60.

43 Чаще всего взятки вымогаются у подозреваемых с помощью силы и принуждения.

Потеря доверия к коммерческим операциям ощущается на уровне межличностных взаимоотношений, на уровне организаций и государства в целом (Wright & Kumar, 2023; Yi et al., 2024; Porcedda, 2023; Sarkar & Shukla, 2024; Tok et al., 2025; Onwuadiamu, 2025). Как отмечали Rainer Bohme и Tyler Moore (2012), большинство людей, пострадавших от киберпреступлений в коммерческих операциях онлайн, никогда больше не участвуют в них из-за страха стать жертвами, в то время как те, кто не знает о киберпреступлениях, с большей вероятностью будут участвовать в коммерческих операциях онлайн. Таким образом, такие киберпреступления отрицательно влияют на желание иностранных граждан заключать сделки с камерунцами в сфере электронной торговли в целом. Это связано с жителями не только Камеруна, но и соседних западноафриканских стран, о чем пишет Yushawu (Abubakari, 2020).

Камерун понес значительные финансовые потери из-за киберпреступлений в сфере электронной коммерции. Поскольку в киберпространстве существует большая свобода выбора[44], потенциальные участники сектора электронной коммерции предпочитают иметь дело с гражданами других стран. Предполагаемый ущерб экономике Камеруна, нанесенный киберпреступлениями в этой сфере в 2021 г., был обнародован Министерством почты и телекоммуникаций, которое является компетентным ведомством по вопросам связи в Камеруне. Согласно отчету министерства по данным ANTIC и ANIF[45], в 2021 г. из-за мошенничества и фишинга Камерун потерял около 12,2 млрд франков CFA.

4.5.2. Необоснованные аресты и задержания в связи с киберпреступностью в сфере электронной коммерции

Произвольные аресты и задержания по подозрению в киберпреступлениях в сфере электронной коммерции, без каких-либо жалоб в нарушение надлежащей правовой процедуры, стали частым явлением в крупных городах Северо-Западного и Юго-Западного регионов Камеруна, таких как Буэа, Баменда и Лимбе. В преамбуле конституции Камеруна[46] четко указано, что ни одно лицо не может быть арестовано или содержаться под стражей иначе, как в порядке, установленном законом. Законом, который определяет такие аресты в Камеруне, является Уголовно-процессуальный кодекс[47]. Вопреки конституционным и процессуальным положениям об аресте и содержании под стражей, большинство подозреваемых в киберпреступлениях подвергаются произвольным арестам без ордера и без соблюдения процедуры задержания на месте преступления[48], предусмотренной УПК. Это может быть связано с тем, что лица, проводящие такой арест, осознают, что они могут быстро получить доход за счет взяток, ряд киберпреступников готовы платить в обмен на свою свободу.

---

44 По определению Lawrence Lessig, это демократия в киберпространстве.

45 Отчет Министерства почты и телекоммуникаций Камеруна за 2021 г. Прим. 24 и 25.

46 Закон № 96-6 от 18 января 1996 г. (с изменениями) Камеруна.

47 Закон № 2005 от 27 июля 2005 г. об Уголовном-процессуальном кодексе Камеруна. Раздел 30

48 Там же. Раздел 31.

Надлежащая правовая процедура является фундаментальным аспектом судебного разбирательства, направленного на защиту гражданских прав. Ее нарушение может привести к аннулированию всего дела[49]. В делах The People v. Mbah Valery[50], The people of Cameroon v. Tamukum Fonjiyang Ferdinand & one other[51] суд первой инстанции города Буэа оправдал и освободил обвиняемых из-за нарушения ряда процессуальных аспектов уголовного судопроизводства, включая незаконные аресты и содержание под стражей. В последнем случае суд первой инстанции постановил, что, хотя личность обвиняемых вызывает сомнения, они должны предстать перед судом свободными людьми. Это произошло из-за серьезных процессуальных ошибок, которые нарушили положения разделов 3 и 8 Уголовно-процессуального кодекса. Это решение не было направлено на поощрение действий обвиняемых, но в значительной степени продемонстрировало важность защиты основных прав человека[52]. Подозреваемые не должны задерживаться силами правопорядка в нарушение их конституционных и юридических прав под предлогом обеспечения соблюдения закона. Большинство таких арестованных не только подвергаются пыткам, но и их финансовые ресурсы вымогаются путем принуждения. Это происходит под предлогом борьбы сотрудников полиции с киберпреступлениями в Камеруне.

Следует пресекать произвольные аресты и задержания без соблюдения надлежащей правовой процедуры, поскольку они нарушают основополагающие принципы гражданской свободы, закрепленные в большинстве международных конвенций и национальных законах. Статья 9 Международного пакта о гражданских и политических правах (МПГПП) 1966 г. запрещает произвольные аресты и задержания, в то время как статья 6 Африканской хартии прав человека и народностей (АХПЧН) 1987 г. гарантирует право на свободу и четко определяет, что лишение этой свободы должно осуществляться по причинам и на условиях, установленных законом. Эти правовые положения применяются в Камеруне в соответствии со ст. 45 Конституции 1996 г. в новой редакции[53].

Случаи незаконных арестов и задержаний в связи с киберпреступлениями в сфере электронной коммерции более распространены в Северо-Западном и Юго-Западном регионах Камеруна по сравнению с другими регионами страны (Abubakari, 2020). Отчасти это объясняется социально-политическим кризисом, охватившим оба региона (Boraine & Leno Doris, 2019). Этот кризис способствовал росту киберпреступлений, связанных с электронной коммерцией, в то время как сотрудники полиции, которые были направлены в эти регионы, воспользовались возможностью незаконно арестовывать и задерживать подозреваемых для получения личной выгоды под предлогом пресечения экономических преступлений. Это привело к откровенному пренебрежению правовыми нормами, гарантирующими гражданские свободы.

---

49 См. Уголовно-процессуальный кодекс Камеруна об абсолютной и относительной недействительности. Разделы 3 и 8. См. также решение Lord Denning по делу United Africa Company Limited (U.A.C) v. Macfoy.

50 CFIB/255/2010(Unreported).

51 (2014) 2 SLR.

52 См. Международный пакт о гражданских и политических правах (МПГПП) и Африканскую хартию прав человека и народов (АХПЧН).

53 Закон № 96-6 от 18 января 1996 г. о Конституции Камеруна. Статья 45.

4.6. Экономические последствия киберпреступности для электронной коммерции

Рост киберпреступлений в сфере электронной коммерции в Камеруне привел к финансовым потерям физических и юридических лиц и к снижению стимулов для участия в операциях электронной коммерции. Это объясняется тем, что страх, вызванный киберпреступлениями, оказывает большее влияние в киберпространстве, поскольку многие люди опасаются стать жертвами таких преступлений (Yokotani & Takano, 2021). Это отражается на спросе на операции электронной коммерции и может значительно снизить оборот и объем производства из-за потери капитала и прибыли в результате действий киберпреступников. Некоторые финансовые потери из-за киберпреступлений в этой сфере могут привести к банкротству. Например, как указано выше, сумма финансовых потерь от киберпреступлений в 2024 г. составила около 12,2 млрд франков CFA. Это оказывает огромное влияние на экономику, и, кроме того, незаконные финансовые доходы, полученные в результате киберпреступлений, связанных с электронной коммерцией, не облагаются налогом.

Все вышеперечисленное препятствует бесперебойному функционированию электронной коммерции в Камеруне. Одной из целей электронной коммерции является обеспечение быстрого оборота. В связи с распространением киберпреступлений в Камеруне возникает огромная проблема, поскольку спрос на услуги электронной торговли сокращается. Потеря доверия из-за киберпреступлений в сфере электронной коммерции также значительно подрывает экономику страны через такие последствия, как усиление инфляции[54], распространение отмывания денег и подделок валюты.

Заключение

В статье рассмотрено влияние киберпреступности на электронную торговлю в Камеруне. Автор отмечает, что большинство киберпреступлений в Камеруне направлено на поддельные транзакции в сфере электронной торговли. Было установлено, что росту числа таких киберпреступлений способствует ряд факторов: экономическая ситуация в Камеруне, легкий доступ к информационно-коммуникационным технологиям, конфликт в Юго-Западном и Северо-Западном регионах страны, стремление граждан вести эпатажный образ жизни. Все это имеет социально-правовые и экономические последствия, а также приводит к распространению других видов преступлений. Результаты проведенного опроса и отчеты Министерства почты и телекоммуникаций демонстрируют, что киберпреступления, связанные с операциями электронной коммерции, в ряде крупных городов Камеруна в основном совершаются молодежью. Ожидается, что число потенциальных правонарушителей в будущем увеличится. Было также обнаружено слабое влияние учреждений, отвечающих за борьбу с киберпреступлениями в стране. Полученные данные свидетельствуют о том, что киберпреступления в сфере электронной коммерции в Камеруне привели к утрате доверия граждан, произвольным арестам и задержаниям в нарушение ряда

[54] Можно заметить, что цены на основные товары в городе Буэа высоки по сравнению с другими городами Камеруна из-за незаконного обогащения, которым в Буэа пользуются в основном молодые люди – мошенники.

международных договоров, конституционных и уголовно-процессуальных положений. В работе отмечено, что большинство подозреваемых избегают судебного преследования, поскольку сотрудники полиции предпочитают брать взятки и отпускать подозреваемых на свободу. Исследование также показало, что указанные киберпреступления подорвали репутацию камерунцев в стране и за рубежом, и многие иностранные граждане отказываются вести с ними онлайн-бизнес. Это объясняется отсутствием надлежащей системы домашних адресов и номеров социального страхования у камерунцев.

Для решения выявленных проблем рекомендуется провести в Камеруне правовые, технологические, социальные и экономические реформы. Необходимо усовершенствовать действующее законодательство, уделив особое внимание процессуальным нормам на этапах расследования и судебного разбирательства по делам о киберпреступлениях, связанных с электронной коммерцией. Закон должен наделить Национальное агентство финансовых расследований (National Financial investigation agency, NFIA) и Национальное агентство информационно-коммуникационных технологий (National Agency for information and communication technologies, NAICT) полномочиями по судебному преследованию случаев киберпреступлений, связанных с электронной коммерцией. Силы правопорядка должны регулярно проходить обучение по вопросам ареста и задержания киберпреступников. Необходимо также предусмотреть стимулы для успешного расследования киберпреступлений, связанных с электронной коммерцией. В случаях коррупции и взяточничества в сфере киберпреступлений должны применяться серьезные санкции. Минимальный уровень заработной платы и шкала оплаты труда в Камеруне должны быть повышены при одновременном создании новых рабочих мест для неработающей молодежи. Следует включить уроки кибербезопасности и электронной коммерции в учебные программы, начиная с начальной школы и заканчивая университетами. В Камеруне необходимо ввести надлежащую систему домашних адресов и номеров социального страхования для идентификации граждан. Следует также усовершенствовать системы управления цифровыми правами и технологии отслеживания.

Список литературы

Abubakari, Y. (2020). The reasons, impacts and limitations of cybercrime policies in Anglophone West Africa: A review. *Social Space Journal*, *12*(3), 45–67.

Alhadidi, I., Nweiran, A., & Hilal, G. (2024). The influence of Cybercrime and legal awareness on the behavior of university of Jordan students. *Heliyon*, *10*(12), e32371. https://doi.org/10.1016/j.heliyon.2024.e32371

Arroyabe, M. F., Arranz, C. F., De Arroyabe, I. F., & De Arroyabe, J. C. F. (2024). Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. *Computers & Security*, *141*, 103826. https://doi.org/10.1016/j.cose.2024.103826

Böhme, R., & Moore, T. (2012). The market for stolen data: Estimating the costs of data breaches. *IEEE Security & Privacy*, *10*(2), 43–49. https://doi.org/10.1109/MSP.2012.40

Boraine, P. A., & Leno Doris, D. N. (2019). The Fight against Cybercrime in Cameroon. *International Journal of Computer (IJC)*, *35*(1), 87–100. https://doi.org/10.53896/ijc.v35i1.1469

Chris, H. et al. (2005). *Criminology*. Oxford: Oxford University Press.

Edwards, M., & Hollely, N. M. (2023). Online sextortion: Characteristics of offences from a decade of community reporting. *Journal of Economic Criminology*, *2*, 100038. https://doi.org/10.1016/j.jeconc.2023.100038

Garner, B. A. (1999). *Black's Law Dictionary* (7th ed.). Minnesota, West Group.

Gupta, A., Matta, P., & Pant, B. (2025). Analyzing the social conduct of users to detect and prevent cybercrime across social networks. *Procedia Computer Science*, *258*, 4269–4278. https://doi.org/10.1016/j.procs.2025.04.676

Higgs, J., & Flowerday, S. (2025a). Detecting cybercrime in online video gaming. *Computers & Security*, *156*, 104528. https://doi.org/10.1016/j.cose.2025.104528

Higgs, J., & Flowerday, S. (2025b). Cybercrime and virtual laundering in video game marketplaces: A Bayesian P-inductive argument. *Technology in Society*, *83*, 102978. https://doi.org/10.1016/j.techsoc.2025.102978

Holt, T. J. (2022). Understanding the state of criminological scholarship on cybercrimes. *Computers in Human Behavior*, *139*, 107493. https://doi.org/10.1016/j.chb.2022.107493

Hornuf, L., Momtaz, P. P., Nam, R. J., & Yuan, Y. (2025). Cybercrime on the ethereum blockchain. *Journal of Banking & Finance*, *175*, *107419*. https://doi.org/10.1016/j.jbankfin.2025.107419

Jansson, K., & von Solms, R. (2011). Phishing for phishing awareness. *Behaviour & Information Technology*, *32*(6), 584–593. https://doi.org/10.1080/0144929x.2011.632650

Lee, S., Kang, I., & Kim, H. (2023). Understanding cybercrime from a criminal's perspective: Why and how suspects commit cybercrimes? *Technology in Society*, *75*, 102361. https://doi.org/10.1016/j.techsoc.2023.102361

Luu, T. J., Samuel, B. M., Jones, M., & Barnes, J. (2025). Exploring how the Dark Triad shapes cybercrime responses. *Personality and Individual Differences*, *244*, 113250. https://doi.org/10.1016/j.paid.2025.113250

Matias, C. F. F. (2025). Access revisited: AI training at the intersection of copyright and cybercrime laws. *Computer Law & Security Review*, *57*, 106149. https://doi.org/10.1016/j.clsr.2025.106149

Onwuadiamu, G. (2025). Cybercrime in Criminology; A Systematic Review of criminological theories, methods, and concepts. *Journal of Economic Criminology*, *8*, 100136. https://doi.org/10.1016/j.jeconc.2025.100136

Orbach, B., & Huang, L. (2018). Con men and their enablers: The anatomy of confidence games. *Social Research: An International Quarterly*, *85*(4), 795–822. https://doi.org/10.1353/sor.2018.0050

Payne, B. K. (2020). *The Handbook of International Cybercrime and Cyberdevidence*. London: Palgrave Macmillian. https://doi.org/10.1007/978-3-319-78440-3

Porcedda, M. G. (2023). Sentencing data-driven cybercrime. How data crime with cascading effects is tackled by UK courts. *Computer Law & Security Review*, *48*, 105793. https://doi.org/10.1016/j.clsr.2023.105793

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being Pursued Online: Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimization. *Criminal Justice and Behavior*, *38*(11), 1149–1169. https://doi.org/10.1177/0093854811421448

Sarefo, S., Mphago, B., & Dawson, M. (2023). An analysis of Botswana's cybercrime legislation. *Procedia Computer Science*, *219*, 1023–1033. https://doi.org/10.1016/j.procs.2023.01.380

Sarkar, G., & Shukla, S. K. (2024). Reconceptualizing online offenses: A framework for distinguishing cybercrime, cyberattacks, and cyberterrorism in the Indian legal context. *Journal of Economic Criminology*, *4*, 100063. https://doi.org/10.1016/j.jeconc.2024.100063

Snidal, D. (2013). Rational Choice and Interntional Relations. In *Handbook of International Relations*. London, Sage. https://doi.org/10.4135/9781446247587.n4

Tok, Y. C., Zheng, D. Y., & Chattopadhyay, S. (2025). A Smart City Infrastructure ontology for threats, cybercrime, and digital forensic investigation. *Forensic Science International Digital Investigation*, *52*, 301883. https://doi.org/10.1016/j.fsidi.2025.301883

Wartiovaara, M. (2011). Rationality, REMM, and Individual Value Creation. *Journal of business Ethics*, *98*(4), 641–648. https://doi.org/10.1007/s10551-010-0643-6

Williamson, O. E. (2008). Outsourcing: Transaction Cost Economics and Supply Chain Management. *Journal of Supply Chain Management*, *44*, 2–82. https://doi.org/10.1111/j.1745-493x.2008.00051.x

Wright, D., & Kumar, R. (2023). Assessing the socio-economic impacts of cybercrime. *Societal Impacts*, *1*(1–2), 100013. https://doi.org/10.1016/j.socimp.2023.100013

Yi, M., Li, J., & Shen, G. (2024). Can targeted poverty alleviation reduce criminal offenses? Empirical evidence from China judgments online data. *China Economic Quarterly International*, *4*(1), 55–68. https://doi.org/10.1016/j.ceqi.2024.03.003

Yokotani, K., & Takano, M. (2021). Predicting cyber offenders and victims and their offense and damage time from routine chat times and online social network activities. *Computers in Human Behavior*, *128*, 107099. https://doi.org/10.1016/j.chb.2021.107099

Yokotani, K., & Takano, M. (2022). Effects of suspensions on offences and damage of suspended offenders and their peers on an online chat platform. *Telematics and Informatics*, *68*, 101776. https://doi.org/10.1016/j.tele.2022.101776

Сведения об авторе

Лекунзе Анумбуандем Бенволио – PhD, преподаватель, кафедра английского права, Университет Буэа
Адрес: Камерун, г. Буэа, а/я 63
E-mail: benleku@yahoo.com
ORCID ID: https://orcid.org/0009-0005-9947-0639

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 27 апреля 2025 г.
Дата одобрения после рецензирования – 9 мая 2025 г.
Дата принятия к опубликованию – 25 сентября 2025 г.
Дата онлайн-размещения – 30 сентября 2025 г.

Research article
UDC 34:004:343.721:004.8
EDN: https://elibrary.ru/tnqlxy
DOI: https://doi.org/10.21202/jdtl.2025.21

Impact of Cybercrime Related Offences on E-commerce in Cameroon: Social-Legal and Economic Consequences

Anoumbuandem Benvolio Lekunze
University of Buea, Buea, Cameroon

Keywords

Cameroon,
cybercrime,
digital technologies,
e-commerce,
fraud,
justice,
law,
scamming,
security,
transactions

Abstract

Objective: to examine the impact of cybercrimes on e-commerce related transactions in Cameroon and evaluate the effectiveness of the legal provisions in force that counteract cyberthreats.

Methods: The research is based on the utilitarian, transaction cost and the rational choice theories. It adopts the qualitative research methodology with the use of the doctrinal method. The author conducted a comprehensive analysis of Cameroon's legal acts in the field of cybersecurity and e-commerce. A survey was carried out between January to April 2025 at Molyko in Buea where 250 sample responses were obtained. Judicial precedents and statistics of the Cameroon Ministry of Posts and Telecommunications were investigated.

Results: It was found that cybercrimes have caused loss of trust and confidence in e-commerce transactions within Cameroon and a declining rate at which people are willing to carry out e-commerce transactions in Cameroon. More than 60% of young persons between the ages of 16 to 35 years in some major Cameroonian cities are either involved in e-commerce related cybercrimes or suffered from them. It was also observed that there is an increase in the rate at which female persons are involved in e-commerce related cybercrimes. The main types of cybercrimes were identified: scamming, phishing, and bank card skimming.

Scientific novelty: it consists in a comprehensive interdisciplinary analysis of the impact of cybercrime on e-commerce in the context of the developing African economy. For the first time, an empirical study of the scale of cybercrime in a specific region of Cameroon was conducted, including

a quantitative assessment of youth involvement in illegal activities. The author has developed a theoretical model that combines the utilitarianism, transaction costs, and rational choice concepts to explain the motivation of cybercriminals. Specific socio-legal factors contributing to the growth of cybercrime in the context of the socio-political crisis were identified.

Practical significance: The study results are of great practical significance for improving the legal, technological, social and economic mechanisms for countering cybercrime in Cameroon. The proposed recommendations include reforming procedural legislation, expanding the powers of specialized agencies, introducing a system of home addresses and social security numbers, raising the minimum wage, and integrating courses on cybersecurity into educational programs. The data obtained can be used by government agencies, the judicial system, educational institutions and international organizations to develop effective strategies to combat cybercrime and develop a secure digital economy.

For citation

Lekunze, A. B. (2025). Impact of Cybercrime Related Offences on E-commerce in Cameroon: Social-Legal and Economic Consequences. *Journal of Digital Technologies and Law, 3*(3), 512–536. https://doi.org/10.21202/jdtl.2025.21

References

Abubakari, Y. (2020). The reasons, impacts and limitations of cybercrime policies in Anglophone West Africa: A review. *Social Space Journal*, *12*(3), 45–67.

Alhadidi, I., Nweiran, A., & Hilal, G. (2024). The influence of Cybercrime and legal awareness on the behavior of university of Jordan students. *Heliyon*, *10*(12), e32371. https://doi.org/10.1016/j.heliyon.2024.e32371

Arroyabe, M. F., Arranz, C. F., De Arroyabe, I. F., & De Arroyabe, J. C. F. (2024). Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. *Computers & Security*, *141*, 103826. https://doi.org/10.1016/j.cose.2024.103826

Böhme, R., & Moore, T. (2012). The market for stolen data: Estimating the costs of data breaches. *IEEE Security & Privacy*, *10*(2), 43–49. https://doi.org/10.1109/MSP.2012.40

Boraine, P. A., & Leno Doris, D. N. (2019). The Fight against Cybercrime in Cameroon. *International Journal of Computer (IJC)*, *35*(1), 87–100. https://doi.org/10.53896/ijc.v35i1.1469

Chris, H. et al. (2005). *Criminology*. Oxford: Oxford University Press.

Edwards, M., & Hollely, N. M. (2023). Online sextortion: Characteristics of offences from a decade of community reporting. *Journal of Economic Criminology*, *2*, 100038. https://doi.org/10.1016/j.jeconc.2023.100038

Garner, B. A. (1999). *Black's Law Dictionary* (7th ed.). Minnesota, West Group.

Gupta, A., Matta, P., & Pant, B. (2025). Analyzing the social conduct of users to detect and prevent cybercrime across social networks. *Procedia Computer Science*, *258*, 4269–4278. https://doi.org/10.1016/j.procs.2025.04.676

Higgs, J., & Flowerday, S. (2025a). Detecting cybercrime in online video gaming. *Computers & Security*, *156*, 104528. https://doi.org/10.1016/j.cose.2025.104528

Higgs, J., & Flowerday, S. (2025b). Cybercrime and virtual laundering in video game marketplaces: A Bayesian P-inductive argument. *Technology in Society*, *83*, 102978. https://doi.org/10.1016/j.techsoc.2025.102978

Holt, T. J. (2022). Understanding the state of criminological scholarship on cybercrimes. *Computers in Human Behavior*, *139*, 107493. https://doi.org/10.1016/j.chb.2022.107493

Hornuf, L., Momtaz, P. P., Nam, R. J., & Yuan, Y. (2025). Cybercrime on the ethereum blockchain. *Journal of Banking & Finance*, *175*, *107419*. https://doi.org/10.1016/j.jbankfin.2025.107419

Jansson, K., & von Solms, R. (2011). Phishing for phishing awareness. *Behaviour & Information Technology*, *32*(6), 584–593. https://doi.org/10.1080/0144929x.2011.632650

Lee, S., Kang, I., & Kim, H. (2023). Understanding cybercrime from a criminal's perspective: Why and how suspects commit cybercrimes? *Technology in Society*, *75*, 102361. https://doi.org/10.1016/j.techsoc.2023.102361

Luu, T. J., Samuel, B. M., Jones, M., & Barnes, J. (2025). Exploring how the Dark Triad shapes cybercrime responses. *Personality and Individual Differences*, *244*, 113250. https://doi.org/10.1016/j.paid.2025.113250

Matias, C. F. F. (2025). Access revisited: AI training at the intersection of copyright and cybercrime laws. *Computer Law & Security Review*, *57*, 106149. https://doi.org/10.1016/j.clsr.2025.106149

Onwuadiamu, G. (2025). Cybercrime in Criminology; A Systematic Review of criminological theories, methods, and concepts. *Journal of Economic Criminology*, *8*, 100136. https://doi.org/10.1016/j.jeconc.2025.100136

Orbach, B., & Huang, L. (2018). Con men and their enablers: The anatomy of confidence games. *Social Research: An International Quarterly*, *85*(4), 795–822. https://doi.org/10.1353/sor.2018.0050

Payne, B. K. (2020). *The Handbook of International Cybercrime and Cyberdevidence*. London: Palgrave Macmillian. https://doi.org/10.1007/978-3-319-78440-3

Porcedda, M. G. (2023). Sentencing data-driven cybercrime. How data crime with cascading effects is tackled by UK courts. *Computer Law & Security Review*, *48*, 105793. https://doi.org/10.1016/j.clsr.2023.105793

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being Pursued Online: Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimization. *Criminal Justice and Behavior*, *38*(11), 1149–1169. https://doi.org/10.1177/0093854811421448

Sarefo, S., Mphago, B., & Dawson, M. (2023). An analysis of Botswana's cybercrime legislation. *Procedia Computer Science*, *219*, 1023–1033. https://doi.org/10.1016/j.procs.2023.01.380

Sarkar, G., & Shukla, S. K. (2024). Reconceptualizing online offenses: A framework for distinguishing cybercrime, cyberattacks, and cyberterrorism in the Indian legal context. *Journal of Economic Criminology*, *4*, 100063. https://doi.org/10.1016/j.jeconc.2024.100063

Snidal, D. (2013). Rational Choice and Interntional Relations. In *Handbook of International Relations*. London, Sage. https://doi.org/10.4135/9781446247587.n4

Tok, Y. C., Zheng, D. Y., & Chattopadhyay, S. (2025). A Smart City Infrastructure ontology for threats, cybercrime, and digital forensic investigation. *Forensic Science International Digital Investigation*, *52*, 301883. https://doi.org/10.1016/j.fsidi.2025.301883

Wartiovaara, M. (2011). Rationality, REMM, and Individual Value Creation. *Journal of business Ethics*, *98*(4), 641–648. https://doi.org/10.1007/s10551-010-0643-6

Williamson, O. E. (2008). Outsourcing: Transaction Cost Economics and Supply Chain Management. *Journal of Supply Chain Management*, *44*, 2–82. https://doi.org/10.1111/j.1745-493x.2008.00051.x

Wright, D., & Kumar, R. (2023). Assessing the socio-economic impacts of cybercrime. *Societal Impacts*, *1*(1–2), 100013. https://doi.org/10.1016/j.socimp.2023.100013

Yi, M., Li, J., & Shen, G. (2024). Can targeted poverty alleviation reduce criminal offenses? Empirical evidence from China judgments online data. *China Economic Quarterly International*, *4*(1), 55–68. https://doi.org/10.1016/j.ceqi.2024.03.003

Yokotani, K., & Takano, M. (2021). Predicting cyber offenders and victims and their offense and damage time from routine chat times and online social network activities. *Computers in Human Behavior*, *128*, 107099. https://doi.org/10.1016/j.chb.2021.107099

Yokotani, K., & Takano, M. (2022). Effects of suspensions on offences and damage of suspended offenders and their peers on an online chat platform. *Telematics and Informatics*, *68*, 101776. https://doi.org/10.1016/j.tele.2022.101776

Author information

Anoumbuandem B. Lekunze – PhD, Lecturer, Department of English Law, University of Buea
Address: PO Box 63, Buea, Cameroon
E-mail: benleku@yahoo.com
ORCID ID: https://orcid.org/0009-0005-9947-0639

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – April 27, 2025
Date of approval – May 9, 2025
Date of acceptance – September 25, 2025
Date of online placement – September 30, 2025