



Научная статья

УДК 34:004:346.6:004.7

EDN: <https://elibrary.ru/lqycmn>

DOI: <https://doi.org/10.21202/jdtl.2025.12>

Псевдонимизация персональных данных пользователей криптоактивов: проблемы правового регулирования в Индонезии

И Команг Оки Маюна



Университет Бравиджая, Маланг, Индонезия

Река Девантара

Университет Бравиджая, Маланг, Индонезия

Патриция Одри Руслиджанто

Университет Бравиджая, Маланг, Индонезия

Ключевые слова

законодательство,
защита персональных
данных,
криптоактивы,
криптовалюта,
персональные данные,
право,
псевдонимизация,
технология блокчейн,
торговля криптоактивами,
цифровые технологии

Аннотация

Цель: анализ возможности обеспечения правовой защиты псевдонимизированных персональных данных пользователей криптоактивов в правовой системе Индонезии.

Методы: в работе применяется комплексный правовой анализ, основанный на изучении действующих нормативных правовых актов Индонезии в сфере защиты персональных данных. Исследование реализовано с использованием законодательного, концептуального и сравнительного методологических подходов, включающих анализ положений индонезийского Закона о защите персональных данных, Общего регламента Европейского союза по защите персональных данных и британского Закона о защите данных.

Результаты: установлено, что псевдонимизация данных пользователей криптоактивов в Индонезии осуществима с правовой точки зрения, однако существующее законодательство содержит существенные пробелы. Действующий Закон о защите персональных данных Индонезии не признает псевдонимизированные данные в качестве отдельной категории персональных данных, подлежащих правовой защите. Выявлена проблематичность реализации правила контроля переводов физическими трейдерами криптоактивов, поскольку дополнительная информация для реидентификации псевдонимизированных данных не хранится отдельно, что увеличивает риски нарушения конфиденциальности.

✉ Корреспондирующий автор

© Маюна И К. О., Девантара Р., Руслиджанто П. О., 2025

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/deed.ru>), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

Научная новизна: проведен комплексный анализ правовых механизмов защиты псевдонимизированных данных в контексте криптовалютных операций. Предложена концептуальная модель совершенствования национального законодательства о защите персональных данных путем включения псевдонимизированных данных в качестве отдельной категории защищаемой информации. Разработаны рекомендации по установлению критериев законной реидентификации псевдонимизированных данных для обеспечения правовой определенности в сфере защиты пользователей криптоактивов.

Практическая значимость: результаты исследования могут служить теоретико-методологической основой для реформирования индонезийского Закона о защите персональных данных и создания эффективного правового механизма защиты пользователей криптоактивов. Предложенные изменения в ст. 4 указанного Закона позволят включить псевдонимизированные данные в перечень защищаемых категорий персональных данных, что обеспечит правовую определенность для участников криптовалютного рынка и повысит уровень защиты их персональных данных в условиях цифровой экономики.

Для цитирования

Маюна, И. К. О., Девантара, Р., Руслиджанто, П. О. (2025). Псевдонимизация персональных данных пользователей криптоактивов: проблемы правового регулирования в Индонезии. *Journal of Digital Technologies and Law*, 3(2), 275–303. <https://doi.org/10.21202/jdtl.2025.12>

Содержание

Введение

1. Концепция защиты персональных данных
 - 1.1. Защита персональных данных
 - 1.2. Значение данных о псевдонимизации
 - 1.3. Значение анонимизированных данных
 - 1.4. Значение агрегированных данных
2. Взаимосвязь между защитой псевдонимизированных данных пользователей криптоактивов и торговлей криптоактивами
3. Регулирование псевдонимизации и реидентификации данных
 - 3.1. Закон Индонезии о защите персональных данных
 - 3.2. Общий регламент ЕС по защите персональных данных
 - 3.3. Закон о защите данных 2018 г.
4. Проблемы защиты псевдонимизированных данных пользователей криптоактивов в Индонезии

Заключение

Список литературы

Введение

В настоящее время мы являемся свидетелями эволюции платежных систем: изначально они опирались на физические деньги, а теперь переходят на электронные. Недавно мир был потрясен появлением криптовалюты, которая используется в качестве способа оплаты в торговых транзакциях (Jati & Zulfikar, 2021). Однако не все страны, включая Индонезию, признают криптовалюту законным платежным средством. Криптовалюта в Индонезии не может использоваться в качестве законного платежного средства, поскольку, согласно ст. 2 Закона о валюте № 7 от 2011 г., официальной валютой Индонезии является рупия (Setiawan et al., 2023). Однако криптовалюта в Индонезии была признана инвестиционным инструментом, как поясняется в ст. 1 Постановления министра торговли № 99 от 2018 г., касающегося торговли фьючерсами на криптоактивы. Поэтому в Индонезии криптовалюта называется криптоактивом (Ulya & Pambudi, 2024).

Транзакции с криптоактивами тесно связаны с обработкой данных в целях псевдонимизации. Когда инвесторы переводят криптоактивы на цифровой кошелек либо в виде активов, либо в виде конвертации в фиатные деньги, транзакция регистрируется в системе блокчейна с использованием адреса кошелька псевдонимизации или публичного адреса. С другой стороны, эти транзакции также регистрируются физическими трейдерами криптоактивов в рамках реализации правила контроля переводов, как предусмотрено п. 1 ст. 38 Регламента № 13 от 2022 г. Агентства по надзору за торговлей товарными фьючерсами, содержащего поправки к соответствующему Регламенту № 8 от 2021 г.

В результате обработка данных псевдонимизации осуществляется физическими трейдерами криптоактивов. Однако дополнительная информация, которая может быть использована для реидентификации, не хранится отдельно от данных псевдонимизации, что увеличивает риск утечки данных. Псевдонимизированные данные остаются связанными с личностью субъекта данных. Более того, исследования показали, что данные, хранящиеся в блокчейнах, могут быть прослежены до физических лиц (субъектов скрытых персональных данных), если они обрабатываются с использованием адекватных технических методов, что потенциально позволяет установить личность субъекта, которому принадлежат псевдонимизированные данные.

К сожалению, Закон о защите персональных данных не признает данные о псевдонимизации в качестве типа данных, подлежащих защите. Поэтому необходимо регулировать данные о псевдонимизации как одну из категорий данных, защищаемых Законом о защите персональных данных, чтобы обеспечить правовые гарантии для инвесторов в криптоактивы.

1. Концепция защиты персональных данных

1.1. Защита персональных данных

Изучение защиты персональных данных требует определения понятия данных. На латыни это *datum* – частица информации. Сбор данных приводит к формированию информации. В контексте персональных данных в разных странах используются разные термины – «персональная информация» или «персональные данные». Однако, по существу, оба термина имеют почти одинаковое значение. Помимо этих терминологических различий, существуют также различия в интерпретации самого понятия

персональных данных¹. В Индонезии используется термин «персональные данные» на основании п. 1 ст. 1 Закона о защите персональных данных²: «Персональные данные – это информация о физическом лице, которая идентифицирует или может идентифицировать это лицо как отдельно, так и в сочетании с другой информацией, прямо или косвенно, через электронные или неэлектронные системы».

Положения Закона о защите персональных данных определяют персональные данные как информацию, которая может быть идентифицирована с помощью электронных или неэлектронных средств. Напротив, в Общем регламенте ЕС по защите персональных данных это различие не оговаривается.

Защита персональных данных включает в себя, по крайней мере, две ключевые концепции: обеспечение физической сохранности персональных данных и установление правовых норм, обеспечивающих гарантии конфиденциальности при использовании данных о субъекте данных. По сути, защита данных тесно связана с обеспечением права на неприкосновенность частной жизни (Yetno, 2021). Алан Вестин также подчеркивал, что конфиденциальность данных – это право отдельных лиц, групп или учреждений самостоятельно определять, когда, как и в каком объеме информация о них будет передаваться или собираться другими лицами³.

На концептуальном уровне выработка всеобъемлющего или стандартного определения конфиденциальности является сложной задачей, поскольку это понятие до сих пор остается предметом постоянных дискуссий среди экспертов. Конфиденциальность означает право человека контролировать сбор, использование, раскрытие и хранение личной информации (Jose, 2023). Концепция неприкосновенности частной жизни была впервые введена Сэмюэлем Уорреном и Луисом Брандейсом, которые заявили, что необходимо защищать такое фундаментальное право человека, как «право на неприкосновенность частной жизни», дав ему следующее определение: «Неприкосновенность частной жизни – это право наслаждаться жизнью и быть оставленным в покое; развитие права в этом направлении было неизбежным и требовало юридического признания» (Anand et al., 2020).

Исходя из этого объяснения, право на неприкосновенность частной жизни включает в себя право наслаждаться жизнью, быть оставленным в покое и добиваться правовой защиты своей частной жизни. Большой словарь индонезийского языка определяет неприкосновенность частной жизни как личную свободу. Уоррен и Брандейс также подчеркивают, что неприкосновенность частной жизни – это право наслаждаться жизнью и быть оставленным в покое, гарантия того, что каждый имеет право сохранять приватность (Dewi, 2017). Таким образом, право на неприкосновенность частной жизни является фундаментальным правом каждого человека на сохранение конфиденциальности и безопасности (Anggen Suari & Sarjana, 2023). Конфиденциальность каждого человека должна быть защищена, но она нарушается, когда личная информация становится достоянием

¹ Djafar, W., Sumigar, B. R. F., & Setianti, B. L. (2016). *Perlindungan Data Pribadi Usulan Pelembagaan Kebijakan Dari Perspektif Hak Asasi Manusia*. Lembaga Studi dan Advokasi Masyarakat.

² Undang – Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Pasal 1 angka 1. (2022). *Lembaran Negara Republik Indonesia*, 196, Tambahan Lembaran Negara Republik Indonesia, 6820.

³ Rollenhagen, L. (2020, September 8). Alan Westin is the father of modern data privacy law. Osano. <https://clck.ru/3MEF5G>

общественности. Таким образом, защита конфиденциальности имеет важное значение. Однако многие эксперты считают, что сложно определить и ограничить понятие конфиденциальности из-за его широкого охвата. В результате во многих странах концепция конфиденциальности совмещена с защитой персональных данных. Это согласуется с современной теорией конфиденциальности, которую Алан Вестин впервые развил в своей книге «Конфиденциальность и свобода», где он пишет следующее: «Конфиденциальность – это право отдельных лиц, групп или учреждений самостоятельно определять, когда, как и в каком объеме информация о них будет передаваться другим» (Pelteret & Ophoff, 2016).

Таким образом, конфиденциальность – это право отдельных лиц, групп или учреждений определять, будут ли данные о них переданы другим сторонам. Эксперты в области права доработали это определение в ответ на развитие информационно-коммуникационных технологий, благодаря которым можно получить доступ к данным о частной жизни человека, а также обрабатывать, собирать и манипулировать данными. В результате один из видов права на неприкосновенность частной жизни получил название «конфиденциальность персональных данных».

Конституция Республики Индонезия от 1945 г. регулирует вопросы защиты прав человека. После внесения в нее поправок регулирование прав граждан стало более всеобъемлющим, так как ранее они рассматривались лишь в общих и кратких формулировках. Поправки 1945 года касались гарантий защиты и соблюдения прав граждан, одним из которых является право на неприкосновенность частной жизни (Asrun, 2016). Защита права на неприкосновенность частной жизни в Конституции Индонезии от 1945 г. не регламентирована в явном виде. Тем не менее защита права на неприкосновенность частной жизни подразумевается п. 1 ст. 28G Конституции, в которой говорится: «Каждый человек имеет право защищать себя, свою семью, честь, достоинство и имущество, которым он владеет, имеет право на чувство безопасности и защищенности от угрозы или страха какого-либо действия или бездействия, затрагивающих права человека»⁴.

Исходя из приведенного выше положения, право на неприкосновенность частной жизни косвенно регулируется этой статьей. Ее интерпретация согласуется с концепциями неприкосновенности частной жизни, рассмотренными ранее, которые включают право на честь, достоинство и собственность, а также право на чувство безопасности и защиту от угроз. Кроме того, гарантии неприкосновенности частной жизни также регулируются п. 1 ст. 29 и ст. 30 Закона № 39 от 1999 г. о правах человека. Однако индонезийские законы и нормативные акты не определяют право на неприкосновенность частной жизни (Rohmansyah et al., 2023).

Право на неприкосновенность частной жизни связано с персональными данными, где они являются одним из элементов, охраняемых законом. Таким образом, каждый имеет право на сохранение конфиденциальности своих персональных данных (конфиденциальность и безопасность) (Priskarini et al., 2019). Европейский суд по правам человека также заявил, что защита персональных данных имеет основополагающее значение. Уважение права человека на неприкосновенность частной жизни регулируется ст. 8 Европейской конвенции о защите прав человека и основных свобод (Sinaga & Putri, 2020). Это также соответствует положениям п. 1 ст. 28G

⁴ Undang – Undang Dasar Negara Republik Indonesia Tahun. (1945). Pasal 28G ayat (1).

Конституции Республики Индонезия от 1945 г., которая защищает персональные данные в рамках права на неприкосновенность частной жизни. Хотя в п. 1 ст. 28G Конституции прямо не упоминается право на неприкосновенность частной жизни, это положение подразумевает гарантию права на неприкосновенность частной жизни (Soraja, 2021).

Кроме того, в комментарии к ст. 26 Закона об электронной информации и сделках (Electronic Information and Transactions, ITE) № 19 от 2016 г. разъясняется, что защита персональных данных является одним из аспектов прав личности (права на неприкосновенность частной жизни) (Priliasari, 2023). Таким образом, защита персональных данных является частью права каждого человека на неприкосновенность частной жизни. Пункт 2 ст. 1 Закона о защите персональных данных гласит: «Защита персональных данных – это комплекс мер по защите персональных данных во время их обработки с целью обеспечения конституционных прав субъектов персональных данных»⁵.

Исходя из этой интерпретации, право на защиту персональных данных является конституционным правом граждан Индонезии, и государство обязано его защищать. Таким образом, защита персональных данных является частью права на неприкосновенность частной жизни, которое неявно защищено пунктом (1) статьи 28G Конституции Республики Индонезия от 1945 г. Персональные данные – это неотъемлемая часть права на конфиденциальность, поскольку их защита является неотъемлемым аспектом права на неприкосновенность частной жизни, гарантированного Конституцией Республики Индонезия от 1945 г.

1.2. Значение данных о псевдонимизации

Большой словарь индонезийского языка определяет псевдоним как имя, используемое для сокрытия подлинной личности. Псевдонимизация данных подразумевает замену идентифицирующих характеристик псевдонимами или другими словами или модификацию данных таким образом, чтобы субъект данных не мог быть идентифицирован напрямую. Присвоение псевдонима может быть связано только с конфиденциальными идентификационными данными (дополнительными данными).

При этом особое внимание уделяется методам, с помощью которых можно заменить, удалить или изменить информацию, идентифицирующую личность, сохраняя эту информацию отдельно. Данные, подвергшиеся псевдонимизации, по-прежнему классифицируются как персональные данные и подпадают под действие Закона о защите данных.

Псевдонимизация начинается с исходных данных, которые затем скрываются, в результате чего создается два набора данных: псевдонимизированные данные и дополнительная информация. Оба набора данных могут быть использованы для восстановления исходных данных. Это означает, что псевдонимизированные данные могут быть связаны с исходными данными субъекта данных с использованием дополнительной информации. Таким образом, псевдонимизация данных строится на принципах защиты данных.

⁵ Undang – Undang Nomor 27, Pasal 1 angka 2. (2022), tentang Perlindungan Data Pribadi, Lembaran Negara Republik Indonesia Tahun, 196, Tambahan Lembaran Negara Republik Indonesia, 6820.

Пункт 5 ст. 4 Общего регламента ЕС по защите персональных данных определяет псевдонимизацию следующим образом: «Псевдонимизация – это процесс обработки персональных данных таким образом, что персональные данные больше не могут быть отнесены к конкретному субъекту данных без использования дополнительной информации, при условии что такая дополнительная информация хранится отдельно и используются технические и организационные меры для обеспечения того, чтобы персональные данные не могли быть отнесены к идентифицированному или идентифицируемому физическому лицу»⁶.

Как объяснялось выше, персональные данные под псевдонимами подпадают под действие Общего регламента ЕС по защите персональных данных. Это определение четко описывает процедуру и подчеркивает, что данные, проходящие процесс псевдонимизации, классифицируются как персональные данные. Данные, используемые в этом процессе, по-прежнему связаны с физическим лицом, которое может быть идентифицировано, что соответствует определению персональных данных. Процесс псевдонимизации предотвращает только прямую идентификацию субъекта данных псевдонимизации (Mourby et al., 2018).

Как описано в п. 5 ст. 4 Общего регламента по защите данных, псевдонимизация – это такая обработка персональных данных, чтобы они не могли быть связаны с конкретным субъектом данных без использования дополнительной информации. Такая дополнительная информация должна храниться отдельно и с соблюдением технических и организационных мер, гарантирующих, что персональные данные не будут связаны с идентифицируемым лицом. Здесь проводится четкое различие между анонимизированными и псевдонимизированными данными. В первом случае принципы защиты данных неприменимы, поскольку субъект не идентифицирован или не может быть идентифицирован. Напротив, вторая категория должна соответствовать принципам защиты данных, поскольку они принадлежат идентифицируемому физическому лицу (Bolognini & Bistolfi, 2017). Это также разъясняется в п. 26 Общего регламента по защите данных, который гласит: «Принципы защиты данных должны применяться к любой информации, касающейся идентифицированного или поддающегося идентификации физического лица; персональные данные, подвергшиеся псевдонимизации, которые могут быть отнесены к физическому лицу с использованием дополнительной информации, следует рассматривать как информацию об идентифицируемом физическом лице...» (Finck & Pallas, 2020).

Таким образом, несмотря на то, что данные псевдонимизации могут быть соотношены с исходными данными их владельца, все субъекты, обрабатывающие и контролирующие персональные данные, должны обеспечить, чтобы любая дополнительная информация, используемая для реидентификации, хранилась отдельно. Это гарантирует, что другие стороны не смогут получить к ней доступ или использовать ее без разрешения для реидентификации исходных данных субъекта, прошедших процесс псевдонимизации (Huang & Zheng, 2023). Таким образом, реидентификацию можно предотвратить, обеспечив, чтобы неавторизованные стороны не получили доступ к дополнительным данным или информации, которую можно использовать для идентификации псевдонимизированных данных (Kohlmayer et al., 2019).

⁶ General Data Protection Regulation (EU GDPR). (2018, May 23). [GDPR-Text.com](https://gdpr-text.com). <https://goo.su/Ke5Byw>

Псевдонимизация представляет собой новый подход к контролю за распространением данных для обеспечения конфиденциальности владельца данных путем применения псевдонимов, которые скрывают взаимосвязь между данными и их владельцем. Цель состоит в осуществлении контроля над потоком информации, передаваемой отдельным лицам, для предотвращения их неправомерного использования. Кроме того, псевдонимизация также позволяет ограничить нежелательное раскрытие данных неавторизованными сторонами. Одним из методов ее реализации является шифрование. Данные, которые подвергаются процессу шифрования, преобразуются в специальные коды, которые генерируют открытый ключ (Suryawijaya, 2023). Псевдонимизация может решить проблемы конфиденциальности (защиты персональных данных), неразглашения и целостности. Область применения псевдонима охватывает данные или информацию, относящиеся к владельцу и псевдониму. Информация о псевдонимах должна быть известна только владельцу или уполномоченной стороне, поскольку с ее помощью можно раскрыть личность субъекта данных (Kumar Rai, 2016).

1.3. Значение анонимизированных данных

Анонимизация – это замена, изменение или удаление отдельных данных или информации таким образом, чтобы их невозможно было реидентифицировать. Следовательно, псевдонимизация отличается от анонимизации тем, что информация, обрабатываемая с помощью псевдонимизации, не удаляется полностью или маскируется, а лишь заменяется псевдонимом, что позволяет реидентифицировать ее с помощью дополнительной информации, хранящейся отдельно. Напротив, при анонимизации не только удаляются имена, но и, как правило, маскируется или полностью удаляется персональная информация, что делает невозможным идентификацию субъекта данных (Hintze & El Emam, 2018).

Псевдонимизация и анонимизация – это два разных понятия, но их часто путают в контексте защиты персональных данных. Из данных, которые подвергаются процессу анонимизации, удаляется любая информация, которая могла бы служить идентификатором субъекта данных. Другими словами, анонимные данные навсегда отключают персональные данные от конкретного идентифицированного или поддающегося идентификации лица. Между тем псевдонимизация не удаляет из данных всю идентифицирующую информацию, а лишь уменьшает связь набора данных с реальной личностью человека (Štarchoň & Pikulík, 2019). Рабочая группа ЕС по ст. 29 также разъяснила, что «псевдонимизация не является методом анонимизации, поскольку псевдонимизация только уменьшает связь набора данных с исходными данными о личности субъекта данных»⁷. Таким образом, данные будут считаться анонимными, если данные, которые подверглись деидентификации, не могут быть изменены или связаны с субъектом, которому они принадлежат (Mourby et al., 2018).

⁷ EU. (1995, October 24). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. <https://clck.ru/3MEFan>

Анонимизация предназначена для предотвращения реидентификации данных или лиц, прошедших процедуру анонимизации. Поэтому анонимные данные не подпадают под действие принципов защиты данных. Это также объясняется в п. 26 Общего регламента, где говорится: «Таким образом, принципы защиты данных не должны применяться к анонимной информации, а именно к информации, которая не относится к идентифицированному или поддающемуся идентификации физическому лицу, или к персональным данным, обезличенным таким образом, что субъект данных не может быть идентифицирован или более не поддается идентификации»⁸.

Итак, анонимные данные не подпадают под принципы защиты персональных данных, поскольку они не могут быть привязаны к конкретному идентифицированному или поддающемуся идентификации лицу. Напротив, данные о псевдонимизации подпадают под действие принципов защиты персональных данных, поскольку они могут быть связаны с идентифицированным или поддающимся идентификации физическим лицом. Таким образом, Общий регламент по защите данных обязывает операторов персональных данных выделять дополнительную информацию, которая может быть использована для реидентификации данных о псевдонимизации. Кроме того, контролер данных также обязан рассмотреть все возможные средства или методы, которые определенные лица могли бы использовать для реидентификации данных псевдонимизации.

1.4. Значение агрегированных данных

Агрегированные данные – это данные, полученные в процессе агрегирования (группировки данных). Агрегирование представляет собой сбор и представление необработанных данных в обобщенной форме для статистического анализа. Агрегированные данные также называются статистическими данными и обычно отображаются в виде таблиц, диаграмм или графиков (Sinulingga, 2022). Таким образом, агрегированные данные не подпадают под защиту персональных данных, поскольку не могут реидентифицировать личность человека. Это также объясняется в п. 26 Общего регламента, в котором говорится: «Настоящее положение не касается обработки такой анонимной информации, в том числе в статистических или исследовательских целях»⁹.

Таким образом, исходя из приведенного выше объяснения, из трех типов данных, а именно псевдонимизированных, анонимизированных и агрегированных данных, только первые подпадают под действие принципов защиты персональных данных. Это связано с тем, что псевдонимизированные данные могут быть идентифицированы как исходные данные владельца, при этом дополнительная информация хранится отдельно.

⁸ Recital 26 General Data Protection Regulation. (2022).

⁹ Там же.

2. Взаимосвязь между защитой псевдонимизированных данных пользователей криптоактивов и торговлей криптоактивами

Криптовалюта – это валюта, не централизованная банками; она создается с использованием технологии компьютерного шифрования, записанной на блокчейн-платформе. Пользователи используют криптовалюту для хранения средств и совершения транзакций, хотя не все страны легализовали криптовалюту в качестве платежного средства в торговых операциях. Например, в соответствии со ст. 2 Закона № 7 от 2011 г. в Индонезии законным платежным средством является рупия ([Setiawan et al., 2023](#)). Таким образом, в Индонезии криптовалюта не является легальной валютой и ее нельзя использовать в качестве платежного средства. Об этом также прямо заявил Банк Индонезии. Кроме того, запрет на использование криптоактивов в качестве платежного средства четко регламентирован Постановлением Банка Индонезии № 20 от 2018 г., касающимся электронных денег ([Chang, 2019](#)).

С другой стороны, криптовалюта может использоваться в Индонезии в качестве инвестиционного инструмента, о чем говорилось выше ([Ulya & Pambudi, 2024](#)). Криптоактивы можно определить как частные активы, использующие систему блокчейна для обеспечения цифровой ценности или договорных прав. Эти активы могут передаваться, храниться или продаваться в электронном виде. В других странах криптоактивы обычно называют криптовалютой, и она может использоваться в качестве виртуальной валюты при совершении сделок купли-продажи ([Pudjastuti & Westra, 2021](#)). Однако в Индонезии криптоактивы могут использоваться только в качестве инвестиционных инструментов.

Криптоактивы – это цифровые валютные системы, защищенные с помощью криптографических методов ([Faozi & Segara Gustanto, 2022](#)). Криптография – это шифрование, которое преобразует текст в знаки или символы. Криптовалюта основана на технологии блокчейн ([Ausop & Aulia, 2018](#)). Таким образом, криптовалюта – это цифровая валюта, которая содержит цифровые данные, связанные с транзакциями пользователей с криптоактивами в системе блокчейн. Криптовалюта неотделима от блокчейна, поскольку последний функционирует как система хранения данных, необходимых тем, кто инвестирует в криптоактивы.

В компьютерных системах существует три типа сетей, один из которых – распределенная сеть. Распределенные системы не подчиняются никакому центральному органу; каждый узел системы является частью сети и напрямую связан с другими узлами ([Suryawijaya, 2023](#)).

Блокчейн реализует распределенную систему, поэтому все узлы сети имеют одинаковые права и обязанности по хранению информации и связаны между собой ([Handoko et al., 2024](#)). Системы, основанные на блокчейне, обеспечивают более высокий уровень прозрачности по сравнению с существующими системами бухгалтерского учета. Благодаря этому изменения видны всем в сети и транзакции не могут быть изменены или удалены после их ввода в блокчейн. Блокчейн обеспечивает прозрачность для всех участников сети, позволяя им видеть транзакции в системе ([Nanda Sari & Gelar, 2024](#)).

Кроме того, блокчейн также реализует децентрализованную систему, которая направлена на устранение участия посредников (третьих лиц), тем самым повышая прозрачность и доверие к системе (Abdul Karim & Hadinata, 2023). Децентрализованный блокчейн, по сути, позволяет каждому подключиться к сети, чтобы иметь доступ к системе (Suryawijaya, 2023). Более того, данные, которые были введены в блокчейн, не могут быть изменены или удалены. Данные в блоках также могут быть прослежены до предыдущих блоков. Транзакции, совершенные в прошлом, нельзя изменить, поэтому их можно легко отследить. Однако безопасность в блокчейн-системах не абсолютна. Это объясняется тем, что такая система прозрачна и децентрализована, поэтому каждый участник может видеть транзакции в сети (Jamwal et al., 2024). Блокчейну по-прежнему посвящено множество исследований, поскольку считается, что безопасность этой технологии еще не идеальна в аспекте защиты данных пользователей, как заявили ученые из Института открытых данных (Utomo, 2022).

Многие пользователи считают, что такая прозрачность не является проблемой для конфиденциальности из-за псевдонимизации, поскольку только пользователи с закрытым ключом могут переписать открытый ключ. При этом в соответствии с концепцией защиты персональных данных контролер должен быть в состоянии гарантировать, что хранящиеся данные остаются конфиденциальными и доступными и что только уполномоченные лица могут получить к ним доступ. Однако на самом деле система противоречит принципам конфиденциальности и доступности, поскольку блокчейн прозрачен и каждый может видеть данные, введенные в него (Tatar et al., 2020). Несмотря на то, что данные в блокчейне псевдонимизированы, исследования показали, что их можно соотнести с конкретными пользователями (скрытыми субъектами персональных данных) с помощью сопоставления данных в сети блокчейн с данными за ее пределами или путем анализа контекста транзакций, которые происходят в блокчейне с использованием сетевого анализа. Более того, реальная личность пользователя также может быть раскрыта при использовании информации вне сети. Кроме того, если дополнительные данные не хранятся отдельно от открытого ключа, они могут раскрыть реальную личность пользователя. Например, в одном из исследований было показано, что возможно идентифицировать владельцев криптоактивов, отслеживая псевдонимизированные адреса кошельков и данные транзакций в блокчейне (Tatar et al., 2020).

Таким образом, криптоактивы тесно связаны с обработкой данных в целях псевдонимизации. В механизме торговых транзакций криптоактивы тесно связаны с процессом псевдонимизации данных. Когда инвесторы осуществляют транзакции (обмен или перевод) криптоактивов, из криптоактивов в фиатные деньги или наоборот, или из одного криптоактива в другой, транзакция вводится в систему блокчейна в виде публичного адреса или адреса кошелька. В результате каждый пользователь блокчейна может видеть транзакции, совершенные инвесторами с криптоактивами, даже если они не знают личность пользователя, создавшего транзакцию, поскольку публичный адрес или адрес кошелька, введенный в блокчейн-систему, псевдонимизированы. Кроме того, трейдер сохраняет транзакцию в виде финансовой записи, о которой сообщает в Агентство по надзору за торговлей товарными фьючерсами (Commodity Futures Trading Regulatory Agency, CoFTRA). Это делается для того, чтобы предотвратить использование транзакций с криптоактивами для совершения преступных действий, таких как отмывание денег.

Таким образом, физическая торговля криптоактивами неотделима от обработки персональных данных при псевдонимизации, особенно в том, что касается защиты данных при псевдонимизации. Это связано с тем, что транзакции по торговле криптоактивами включают псевдонимизированные адреса кошельков, записанные в системе блокчейна. Кроме того, трейдеры обязаны применять принцип «Знай своего клиента» (KYC), что предполагает сбор персональных данных клиентов в рамках программ по борьбе с отмыванием денег и усилий по предотвращению финансирования терроризма и распространения оружия массового уничтожения. Таким образом, действия по сбору персональных данных трейдерами криптоактивов могут привести к получению «дополнительной информации», которая может быть использована для реидентификации данных псевдонимизации пользователей криптоактивов (Atikah, 2023).

Кроме того, продавцы физических криптоактивов собирают адреса псевдонимных кошельков в рамках правила контроля переводов. Этот нормативный акт требует от поставщиков услуг виртуальных активов (трейдеров криптоактивами) собирать, хранить и передавать определенную информацию об отправке и получении активов в каждой проводимой транзакции, включая те, которые пересекают границы юрисдикции (Maulana, 2024). Это соответствует правилам торговли криптоактивами в сети, когда публичный адрес пользователя или адрес кошелька записывается в блокчейне и на платформе, где осуществляются транзакции по торговле криптоактивами. Это повышает риск того, что публичный адрес клиента криптоактивов или адрес кошелька будет реидентифицирован с помощью дополнительной информации, полученной и собранной трейдером криптоактивов в рамках реализации принципа «знай своего клиента» (Alfin et al., 2024).

Итак, персональные данные обрабатываются в псевдонимизированной форме физическими трейдерами криптоактивов. Однако реализация правила контроля переводов не учитывает принцип защиты персональных данных в форме псевдонимизации, когда «дополнительная информация», которая может быть использована для реидентификации, должна храниться отдельно. Таким образом, торговля криптоактивами тесно связана с защитой данных инвесторов. Следовательно, нормативные акты должны гарантировать защиту обработки данных о псевдонимизации инвесторов в процессе транзакции с криптоактивами.

3. Регулирование псевдонимизации и реидентификации данных

3.1. Закон Индонезии о защите персональных данных

Защита персональных данных является конституционным правом граждан Индонезии. Это также подтверждается п. 2 ст. 1 Закона о защите персональных данных, в котором говорится, что защита персональных данных – это всеобщие усилия по защите персональных данных при их обработке для обеспечения конституционных прав субъектов персональных данных. Персональные данные, о которых идет речь, относятся к данным о физических лицах, которые идентифицируются или могут быть идентифицированы отдельно или в сочетании с другой информацией, прямо или косвенно, с помощью электронных или неэлектронных систем. Основываясь на разъяснении п. 1 ст. 1 Закона о защите персональных данных, в данной работе мы попытались обобщить значение данных для псевдонимизации. Псевдонимизация данных подразумевает изменение или замену

идентифицирующих характеристик данных на псевдоним таким образом, что это не позволяет идентифицировать субъекта данных напрямую без помощи дополнительной информации, хранящейся отдельно.

К сожалению, Закон о защите персональных данных не регулирует использование псевдонимов в качестве одного из видов данных, которые подлежат защите. Это видно из положений п. 1 ст. 4 указанного закона, который разделяет персональные данные на два типа: конкретные и общие. Конкретные персональные данные включают в себя данные о состоянии здоровья, судимости, детях, личных финансах; биометрические, генетические и другие данные, предусмотренные законодательством. Общие персональные данные включают полное имя, пол, национальность, вероисповедание, семейное положение и/или персональные данные, объединенные для идентификации личности (Adhiwisaksana & Allagan, 2023). Однако оба этих типа не включают данные о псевдонимизации в качестве части персональных данных, которые подлежат защите.

Несмотря на то, что подп. f п. 3 ст. 4 Закона о защите персональных данных включает «персональные данные, объединенные для идентификации личности», разъяснение к подп. f п. 3 ст. 4 указанного закона включает только номера сотовых телефонов и IP-адреса. Под термином «персональные данные, объединенные для идентификации личности» подразумевается, что данные используются для идентификации или установления связи с индивидуальным владельцем персональных данных. Таким образом, они принципиально отличаются от данных для псевдонимизации, которые не предназначены для идентификации или установления связи с физическими лицами. Напротив, данные псевдонимизации предназначены для сокрытия личности субъекта данных, что делает невозможной его реидентификацию без использования дополнительной информации, которая хранится отдельно.

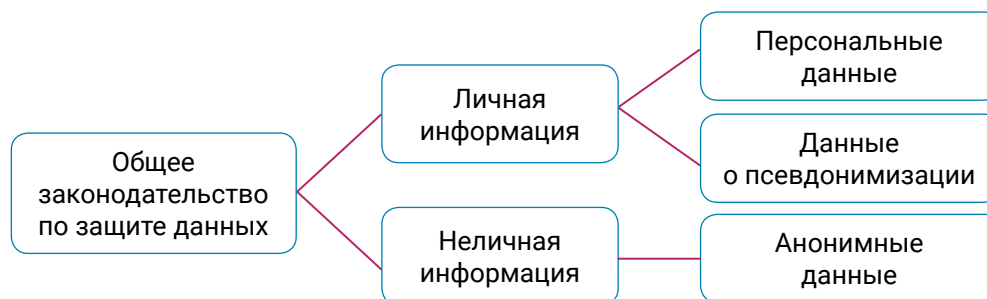
Более того, Закон о защите персональных данных не регулирует критерии реидентификации, которые необходимы для псевдонимизации данных. Этот закон также не регулирует требования к обработке данных о псевдонимизации, которые были реидентифицированы и считаются действительными. Он не рассматривает данные о псевдонимизации как данные, на которые распространяются принципы защиты данных. Таким образом, Закон о защите персональных данных не регулирует реидентификацию и обработку реидентифицированных персональных данных, что может привести к нарушениям прав в области персональных данных.

3.2. Общий регламент ЕС по защите персональных данных

Общий регламент Европейского союза по защите данных (далее – GDPR) включает в себя положения о деидентификации, одно из которых касается псевдонимизации. Регламент вводит концепцию псевдонимизации, что способствовало популяризации идеи псевдонимизации данных, которая относится к сфере персональных и анонимных данных. Определение информации о псевдонимизации подчеркивает, что хранение и защита дополнительной информации должны осуществляться отдельно. Это положение разъясняется в п. 5 ст. 4 GDPR (Joo & Kwon, 2023).

В п. 1 ст. 4 GDPR персональные данные определяются как «любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу («субъекту данных»); идентифицируемое физическое лицо – это лицо, которое может быть идентифицировано прямо или косвенно, в частности, путем ссылки на идентификатор, такой как имя, идентификационный номер, данные о местоположении,

онлайн-идентификатор или на один или несколько факторов, специфичных для физической, физиологической, генетической, ментальной, экономической, культурной или социальной идентичности данного физического лица» (Imakura et al., 2023). Ниже на рисунке представлены персональные данные, на которые распространяются принципы защиты данных в соответствии с GDPR (Joo & Kwon, 2023):



Персональные данные, отвечающие принципам защиты данных

Источник: (Joo & Kwon, 2023).

Общий регламент ЕС защищает данные о псевдонимизации, которые не считаются анонимными, поскольку они могут быть идентифицированы или реидентифицированы с использованием дополнительной информации, которая должна храниться отдельно (Limniotis, 2021). Регламент устанавливает принципы защиты данных для псевдонимизации, как описано в п. 26 GDPR: «Принципы защиты данных должны применяться к любой информации, касающейся идентифицированного или поддающегося идентификации физического лица; персональные данные, подвергшиеся псевдонимизации, которые могут быть отнесены к физическому лицу с использованием дополнительной информации, следует рассматривать как информацию о физическом лице, позволяющую установить его личность»¹⁰. Европейский союз включает данные о псевдонимизации в сферу персональных данных, поэтому они защищены законом (Wahyuningtyas, 2024).

Однако Регламент не содержит принципов защиты анонимных данных, как поясняется в п. 26 GDPR: «Таким образом, принципы защиты данных не должны применяться к анонимной информации, а именно к информации, которая не относится к идентифицированному или поддающемуся идентификации физическому лицу, или к персональным данным, обезличенным таким образом, что субъект данных не может быть идентифицирован или более не поддается идентификации»¹¹. Это связано с тем, что, по сути, анонимные данные предназначены для предотвращения реидентификации, а значит, данные, прошедшие процесс анонимизации, не могут быть связаны или реидентифицированы с конкретным человеком (Dat & An, 2024).

Таким образом, ст. 29 GDPR обязывает контролеров данных выделять дополнительную информацию, которая может быть использована для привязки персональных данных, подвергшихся псевдонимизации. Кроме того, контролер должен также учитывать все средства или методы, которые могут быть использованы для реидентификации псевдонимизированных данных. Такой порядок представляет

¹⁰ Recital 26 General Data Protection Regulation. (2022).

¹¹ Там же.

собой форму правовой защиты в случае обработки данных с псевдонимизацией (Finck & Pallas, 2020). К сожалению, Общий регламент ЕС по защите данных не содержит дополнительных положений, касающихся критериев реидентификации данных с псевдонимизацией, которые считаются действительными. С другой стороны, он обязывает страны-участницы устанавливать правовые нормы, применимые к нарушениям положений Регламента, как предусмотрено п. 1 ст. 84 GDPR.

3.3. Закон о защите данных 2018 г.

Общий регламент ЕС по защите данных (GDPR) распространяется на страны Европейского союза и требует включения его положений в соответствующие национальные законы о защите персональных данных. Таким образом, Регламент обязывает страны-участницы установить правовые нормы, применимые к нарушениям его положений, как предусмотрено п. 1 ст. 84 GDPR. Кроме того, страны-участницы должны также поощрять разработку этических кодексов, которые могут способствовать внедрению Регламента; это относится, в частности, к псевдонимизации данных, как указано в подп. d п. 2 ст. 40 GDPR. В связи с этим в Великобритании были приняты нормы защиты данных, а именно Закон о защите данных 2018 г., который регулирует реидентификацию данных с псевдонимизацией. Пункт 2 ст. 171 Закона о защите данных Великобритании от 2018 г. определяет деидентификацию и реидентификацию следующим образом:

«(a) персональные данные считаются «деидентифицированными», если они были обработаны таким образом, что их нельзя отнести к конкретному субъекту данных без использования дополнительных данных;

(b) лицо «реидентифицирует» информацию, если оно предпринимает шаги, в результате которых информация перестает быть деидентифицированной по смыслу подпункта (a)»¹².

Лицо, которое реидентифицирует обезличенную (псевдонимизированную) информацию, составляющую персональные данные, без согласия контролера, ответственного контролера или надзорного органа, нарушает правила обработки персональных данных, как установлено п. 1 ст. 171 Закона о защите данных от 2018 г. Таким образом, положения пп. 1 и 2 ст. 171 Закона о защите данных от 2018 г. относятся к псевдонимизации, как указано в п. 5 ст. 4 GDPR. Реидентификация псевдонимизированных данных является нарушением правил обработки персональных данных.

Однако Закон о защите данных 2018 г. предусматривает критерии для реидентификации, которые считаются действительными. Один из них отвечает общественным интересам, включая цели предотвращения или раскрытия преступлений, когда это требуется или разрешено законом или постановлением суда, а также в общественных интересах, как предусмотрено п. 3 ст. 171 указанного закона. Кроме того, идентификация считается действительной, если она основана на разумной уверенности или предназначена для специальных целей, таких как академические исследования, как предусмотрено п. 4 ст. 171. Данный закон также регулирует нарушения, связанные с обработкой реидентифицированных персональных данных, если выясняется, что такая обработка осуществлялась без разрешения ответственной стороны, а реидентификация нарушает положения п. 1 ст. 171.

¹² Data Protection Act. (2018), Article 171 Paragraph (2).

Закон о защите данных 2018 г. также содержит критерии для обработки реидентифицированных персональных данных, которые считаются законными, а именно в общественных интересах, включая цели предотвращения или раскрытия преступлений, требуемые или разрешенные законом или постановлением суда, и в иных общественных интересах, как регулируется п. 6 ст. 171 указанного закона. Кроме того, обработка реидентифицированных персональных данных считается законной, если она основана на разумных основаниях и для конкретных целей, таких как академические исследования, как это предусмотрено в п. 7 ст. 171. Однако п. 7 ст. 171 не включает «проверку эффективности» в качестве одного из критериев, тогда как в п. 4 ст. 171 проверка эффективности включена в критерии реидентификации, которые считаются действительными.

4. Проблемы защиты псевдонимизированных данных пользователей криптоактивов в Индонезии

Право на неприкосновенность частной жизни – это право каждого человека жить без вмешательства в его частную жизнь, будь то со стороны других людей или государства. Таким образом, государство несет ответственность и обязано регулировать и признавать эти права. Неприкосновенность частной жизни, как неотъемлемое право человека, может быть разделена на несколько видов, одним из которых является конфиденциальность информации. Информация, считающаяся частной, может быть представлена в различных формах в зависимости от ее предполагаемого использования. Симсон Гарфинкель делит ее на пять типов: личная информация, приватная информация, информация для удостоверения личности, псевдонимная или анонимная информация, агрегированная информация (Syailendra et al., 2024).

Право на неприкосновенность частной жизни косвенно регулируется п. 1 ст. 28G Конституции Республики Индонезия 1945 г. Защита персональных данных тесно связана с правом на неприкосновенность частной жизни, поскольку представляет собой один из видов этого права. Таким образом, защита персональных данных является частью прав человека, как это предусмотрено в п. 1 ст. 28G Конституции Республики Индонезия 1945 г. (Priskarini et al., 2019). Поэтому Индонезия приняла Закон о защите персональных данных как форму защиты прав человека, в частности права на неприкосновенность частной жизни.

К сожалению, Закон о защите персональных данных не может в полной мере обеспечить правовую защиту в отношении обработки данных, связанных с псевдонимизацией, особенно для пользователей криптоактивов. Это связано с тем, что указанный закон не регулирует данные, связанные с псевдонимизацией, как один из видов данных, которые подлежат защите. Таким образом, Закон о защите персональных данных, в частности ст. 4, которая регулирует типы персональных данных, пока не предусматривает регулирование «данных о псевдонимизации» как защищенного типа данных. Несмотря на то, что в подп. f п. 3 ст. 4 говорится о «совокупности персональных данных для идентификации лица», комментарий к нему упоминает только номера мобильных телефонов и IP-адреса. Кроме того, данные псевдонимизации предназначены не для идентификации, а для сокрытия личности субъекта, что делает невозможной прямую идентификацию без использования дополнительной информации, хранящейся отдельно.

Таким образом, Закон о защите персональных данных не может полностью гарантировать защиту персональных данных пользователей криптоактивов путем

обработки персональных данных в виде псевдонимизации. Транзакции с криптоактивами тесно связаны с обработкой персональных данных в форме псевдонимизации, поскольку транзакции (обмен или передача) криптоактивов, будь то из криптоактивов в фиатные деньги или наоборот, а также из одного криптоактива в другой, будут записываться в блокчейн-системе как публичный адрес под псевдонимом или адрес кошелька.

Кроме того, транзакция также записывается или сохраняется трейдером криптоактивов в виде имен отправителей и пользователей, адресов кошельков отправителя и получателя, а также адресов отправителя и пользователя в рамках правила контроля переводов. Это согласуется с правилами торговли криптоактивами в сети, когда публичный адрес пользователя/адрес кошелька записывается в блокчейн-системе и на платформе, которую пользователи используют для торговых транзакций.

Такая обработка информации представляет риск, поскольку публичный адрес клиента криптоактивов или адрес кошелька может быть реидентифицирован с использованием дополнительной информации, полученной и собранной трейдером криптоактивов в рамках реализации принципа «знай своего клиента» (Alfin et al., 2024). Таким образом, сбор персональных данных в виде данных псевдонимизации осуществляется вместе со сбором дополнительной информации, которая может быть использована для реидентификации данных псевдонимизации пользователей криптоактивов (Atikah, 2023).

Защита персональных данных в электронных системах должна осуществляться при соблюдении прав владельцев персональных данных на неприкосновенность частной жизни, поскольку персональные данные являются конфиденциальными. Таким образом, организаторы электронных систем, в данном случае физические торговцы криптоактивами, должны защищать электронную информацию, собранную в рамках применения правила контроля переводов или принципа «знай своего клиента» (Utomo, 2020). К сожалению, Закон о защите персональных данных не может гарантировать защиту при обработке персональных данных в форме псевдонимизации, поскольку, по сути, он не регулирует псевдонимизацию данных как один из видов данных, подлежащих защите. Это создает проблему для защиты данных псевдонимизации для пользователей криптоактивов, поскольку законодательство не предусматривает механизмов правовой защиты для обработки персональных данных в рамках псевдонимизации данных.

Следовательно, чтобы обеспечить правовую защиту пользователей криптоактивов, необходимо изменить Закон о защите персональных данных в части регулирования типов данных, которые подлежат защите. Это согласуется с теорией превентивной правовой защиты, выдвинутой Филипусом М. Хаджоном (Philipus M. Hadjon), которая предполагает установление правил, способных защитить каждого гражданина (Tirtakoesoemah & Arafat, 2019). Необходимо установить правила, регулирующие использование псевдонимов в качестве одного из видов данных, в отношении которых указанный закон гарантирует правовую защиту, предоставляемую государством пользователям криптоактивов при обработке персональных данных в форме псевдонимизации.

Это положение поможет обеспечить правовую определенность в отношении правовой защиты пользователей криптоактивов за счет обработки персональных данных в виде псевдонимизации, выполняемой физическими лицами, торгующими криптоактивами. В настоящее время пользователи криптоактивов не получают

правовой защиты в этой сфере, поскольку применяется правило контроля переводов. Кроме того, дополнительная информация, которая используется для идентификации данных псевдонимизации, не хранится отдельно, что делает ее уязвимой для использования сторонами, не уполномоченными на незаконную реидентификацию данных псевдонимизации ([Ayunda, 2022](#)).

По сообщению на веб-сайте Министерства торговли Республики Индонезия, число пользователей криптоактивов в стране выросло до 21,27 млн человек в период с февраля 2021 г. по сентябрь 2024 г. Новостные СМИ сообщали о предполагаемой утечке личной информации 13 млн пользователей Binance, включая имена, электронные письма, номера телефонов и адреса проживания. В настоящее время информация об утечке данных о псевдонимизации в Индонезии не подтверждена. Однако разглашение персональных данных в виде имен, адресов электронной почты и телефонных номеров может стать существенной причиной утечки данных о псевдонимизации. Эти данные могут быть использованы в качестве дополнительной информации для реидентификации лиц, которым принадлежат псевдонимизированные данные.

Кроме того, реидентификация псевдонимизированных данных также может привести к взлому личных адресов пользователей криптоактивов (компрометация закрытого ключа). Это означает несанкционированный доступ определенного лица к закрытому ключу пользователя криптоактивов. Расследование показало, что произошло 19 случаев компрометации секретного ключа, приведших к финансовым потерям в размере 641,54 млн долларов в 2022 г. и 231,00 млн долларов в 2023 г. ([Multazam et al., 2024](#)). Очевидно, что Индонезии необходимо создать надежную и скоординированную правовую систему в области информационных технологий для достижения правовой определенности в отношении защиты пользователей криптоактивов путем обработки персональных данных в форме псевдонимизации.

Это согласуется с теорией правовой конвергенции, выдвинутой Данриванто Будхиджанто (Danrivanto Budhijanto) на основе теории конвергенции 4C. Теория правовой конвергенции постулирует, что в цифровую эпоху технологические, экономические и правовые переменные в человеческих отношениях унифицируются. Ученый подчеркивает необходимость разработки законов как на национальном, так и на международном уровне, с учетом технологических достижений ([Rizko Ramadoni et al., 2021](#)). Исследования показали, что данные в блокчейнах могут быть соотнесены с физическими лицами (скрытые субъекты персональных данных) с помощью соответствующих технических средств. Это можно сделать, подключив данные, доступные в сети блокчейн, к данным за пределами сети и проанализировав контекст транзакций, которые происходят в блокчейне, с помощью сетевого анализа. Кроме того, реальная личность пользователя может быть раскрыта при использовании информации вне сети ([Jamwal et al., 2024](#)).

Таким образом, необходимо регламентировать данные о псевдонимизации в Законе о защите персональных данных, чтобы гарантировать правовую определенность в отношении правовой защиты обработки данных о псевдонимизации пользователей криптоактивов. Отсутствие такого регулирования создает проблему для пользователей криптоактивов, препятствуя им в получении правовой защиты в отношении обработки данных в форме псевдонимизации.

Закключение

Защита персональных данных является частью права на неприкосновенность частной жизни, которое косвенно регулируется п. 1 ст. 28G Конституции Республики Индонезия 1945 г. среди других фундаментальных прав человека. Поэтому государство должно обеспечивать защиту обработки данных своих граждан, в том числе пользователей криптоактивов. Операции по торговле физическими криптоактивами тесно связаны с обработкой данных под псевдонимами. Транзакции с криптоактивами внутри сети в виде обменов или переводов записываются в блокчейн-систему как адрес кошелька или публичный адрес. Кроме того, трейдеры физическими криптоактивами также регистрируют и хранят детали транзакций, такие как имена отправителя и получателя, адреса кошельков отправителя и получателя, а также адреса отправителя и получателя, в рамках своих обязательств по применению правила контроля переводов.

В принципе, защита данных о псевдонимизации требует, чтобы дополнительная информация, которая может быть использована для реидентификации данных о псевдонимизации, хранилась отдельно. Однако на практике физические трейдеры криптоактивов занимаются обработкой данных о псевдонимизации пользователей криптоактивов. К сожалению, Закон о защите персональных данных не регулирует использование псевдонимов в качестве типа данных, на которые распространяются принципы защиты персональных данных. Кроме того, физические лица, торгующие криптоактивами, обязаны применять принцип «знай своего клиента».

Таким образом, ст. 4 Закона о защите персональных данных необходимо изменить, добавив «данные для псевдонимизации» в качестве одного из видов персональных данных. Это дало бы пользователям криптоактивов юридическую определенность в отношении правовой защиты при обработке персональных данных в качестве данных для псевдонимизации. Кроме того, Закон о защите персональных данных должен учитывать критерии реидентификации псевдонимизированных данных, которые считаются действительными, чтобы гарантировать юридическую определенность для пользователей криптоактивов. Таким образом, правовая защита пользователей криптоактивов при обработке персональных данных в форме псевдонимизации станет невозможной, поскольку будет регулироваться нормативными актами.

Список литературы

- Abdul Karim, M. S., & Hadinata, F. (2023). Implikasi Filosofis Desentralisasi Bitcoin Dalam Perspektif Empire Negri-Hardt. *Jaqfi: Jurnal Aqidah dan Filsafat Islam*, 8(1), 48–60. (In Indonesian). <https://doi.org/10.15575/jaqfi.v8i1.26627>
- Adhiwisaksana, M. F., & Allagan, T. M. P. (2023). Competent Forum and the Applicable Law in Personal Data Protection With Foreign Element. *Indonesian Journal of International Law*, 20(3), 442–470. <https://doi.org/10.17304/ijil.vol20.3.2>
- Alfin, M. H., Idayanti, S., & Rahayu, K. (2024). Regulasi Dan Mekanisme Jual Beli Aset Kripto Di Indonesia. *Jurnal Ilmiah Mahasiswa Ekonomi Syariah (JIMESHA)*, 3(2), 179–188. (In Indonesian). <https://doi.org/10.36908/jimesha.v3i2.312>
- Anand, G., Hernoko, A. Y., & Dharmadji, A. G. (2020). The Urgency of Enacting Personal Data Protection Law As a Patronage From the Development of Communication and Information Technology in Indonesia. *Perspektif*, 25(1), 54–62. <https://doi.org/10.30742/perspektif.v25i1.750>
- Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, 6(1), 132–142. (In Indonesian). <https://doi.org/10.38043/jah.v6i1.4484>

- Asrun, A. M. (2016). Hak Asasi Manusia Dalam Kerangka Negara Hukum: Catatan Perjuangan di Mahkamah Konstitusi. *Jurnal Cita Hukum*, 4(1), 133–154. (In Indonesian). <https://doi.org/10.15408/jch.v4i1.3200>
- Atikah, I. (2023). Perlindungan Hukum Pelanggan Aset Kripto Transaksi Perdagangan Berjangka Komoditi Indonesia. *SALAM: Jurnal Sosial Dan Budaya Syar-I*, 10(2), 497–514. (In Indonesian). <https://doi.org/10.15408/sjsbs.v10i2.31691>
- Ausop, A. Z., & Aulia, E. S. N. (2018). Teknologi Cryptocurrency Bitcoin Untuk Investasi Dan Transaksi Bisnis Menurut Syariat Islam. *Jurnal Sositeknologi*, 17(1), 74–92. (In Indonesian). <https://doi.org/10.5614/sostek.itbj.2018.17.1.8>
- Ayunda, R. (2022). Personal Data Protection to E-Commerce Consumer: What Are the Legal Challenges and Certainties? *Law Reform*, 18(2), 144–163. <https://doi.org/10.14710/lr.v18i2.43307>
- Bolognini, L., & Bistolfi, C. (2017). Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation. *Computer Law and Security Review*, 33(2), 171–181. <https://doi.org/10.1016/j.clsr.2016.11.002>
- Chang, S. E. (2019). Legal Status of Cryptocurrency in Indonesia and Legal Analysis of the Business Activities in Terms of Cryptocurrency. *Brawijaya Law Journal*, 6(1), 76–93. <https://doi.org/10.21776/ub.blj.2019.006.01.06>
- Dat, H. L. N. T., & An, C. T. T. (2024). The Regulation of Data Transmission in the Digital Era: From the European Union's Perspective and Implications for Vietnam. *Vietnamese Journal of Legal Sciences*, 11(2), 1–13. <https://doi.org/10.2478/vjls-2024-0007>
- Dewi, S. (2017). Model Regulation for Data Privacy in the Application of Biometric Smart Card. *Brawijaya Law Journal*, 4(1), 117–128. <https://doi.org/10.21776/ub.blj.2017.004.01.06>
- Faozi, M., & Segara Gustanto, E. (2022). Kripto, Blockchain, Bitcoin, dan Masa Depan Bank Islam: Sebuah Literatur Review. *Quranomic: Jurnal Ekonomi Dan Bisnis Islam*, 1(2), 127–151. (In Indonesian).
- Finck, M., & Pallas, F. (2020). They who must not be identified – distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, 10(1), 11–36. <https://doi.org/10.1093/idpl/ipz026>
- Handoko, R. M., Aulyansyah, B., Trisna, A., & Delon, R. (2024). Implementasi Blockchain Untuk Keamanan Sistem Pembayaran Digital dan Optimasi Transaksi Keuangan (Studi Kasus Industri Fintech di Indonesia). *Teknik: Jurnal Ilmu Teknik dan Informatika*, 4(2), 64–74. (In Indonesian).
- Hintze, M., & El Emam, K. (2018). Comparing the benefits of pseudonymisation and anonymisation under the GDPR. *Journal of Data Protection and Privacy*, 2(2), 145–158. <https://doi.org/10.69554/qsst9019>
- Huang, T., & Zheng, S. (2023). Using Differential Privacy to Define Personal, Anonymous, and Pseudonymous Data. *IEEE Access*, 11, 109225–109236. <https://doi.org/10.1109/ACCESS.2023.3321578>
- Imakura, A., Sakurai, T., Okada, Y., Fujii, T., Sakamoto, T., & Abe, H. (2023). Non-readily identifiable data collaboration analysis for multiple datasets including personal information. *Information Fusion*, 98, 101826. <https://doi.org/10.1016/j.inffus.2023.101826>
- Jamwal, S., Cano, J., Lee, G. M., Tran, N. H., & Truong, N. (2024). A survey on Ethereum pseudonymity: Techniques, challenges, and future directions. *Journal of Network and Computer Applications*, 232, 104019. <https://doi.org/10.1016/j.jnca.2024.104019>
- Jati, Hardian Satria, Zulfikar, A. A. (2021). Transaksi Cryptocurrency Perspektif Hukum Ekonomi Syariah. *Al-Adalah: Jurnal Hukum Dan Politik Islam*, 6(2), 137–148. (In Indonesian). EDN: <https://elibrary.ru/mrkhni>. DOI: <https://doi.org/10.35673/ajmpi.v6i2.1616>
- Joo, M. H., & Kwon, H. Y. (2023). Comparison of personal information de-identification policies and laws within the EU, the US, Japan, and South Korea. *Government Information Quarterly*, 40(2), 101805. <https://doi.org/10.1016/j.giq.2023.101805>
- Jose, N. S. (2023). Information and Communication Technologies and the Right to Informational Privacy in Health Care: A Comprehensive Analysis. *Brawijaya Law Journal*, 10(1), 34–58. <https://doi.org/10.21776/ub.blj.2023.010.01.03>
- Kohlmayer, F., Lautenschläger, R., & Prasser, F. (2019). Pseudonymization for research data collection: Is the juice worth the squeeze? *BMC Medical Informatics and Decision Making*, 19(1), 1–7. <https://doi.org/10.1186/s12911-019-0905-x>
- Kumar Rai, B. (2016). Pseudonymization Techniques for Providing Privacy and Security in EHR. *International Journal of Emerging Trends & Technology in Computer Science*, 5(4).
- Limnietis, K. (2021). Cryptography as the means to protect fundamental human rights. *Cryptography*, 5(4), 1–33. <https://doi.org/10.3390/cryptography5040034>
- Maulana, E. T. (2024). Regulasi Travel Rule Terhadap Transaksi Aset Virtual Lintas Batas Dalam Konteks Decentralized Finance Di Indonesia: Studi Banding Terhadap Markets In Crypto-Assets (Mica) Di Uni Eropa. *JURNAL RECTUM: Tinjauan Yuridis Penanganan Tindak Pidana*, 6(3), 565–584. (In Indonesian).

- Mourby, M., Mackey, E., Elliot, M., Gowans, H., Wallace, S. E., Bell, J., Smith, H., Aidinlis, S., & Kaye, J. (2018). Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK. *Computer Law and Security Review*, 34(2), 222–233. <https://doi.org/10.1016/j.clsr.2018.01.002>
- Multazam, M. T., Phahlevi, R. R., Purnomo, M. I., Purwaningsih, S. B., & Sabirov, B. (2024). Securing Blockchain Enterprises: Legal Due Diligence Amidst Rising Cyber Threats. *Padjadjaran Jurnal Ilmu Hukum (Journal of Law)*, 11(1), 26–52. <https://doi.org/10.22304/pjih.v11n1.a2>
- Nanda Sari, A., & Gelar, T. (2024). Blockchain: Teknologi Dan Implementasinya. *Jurnal Mnemonic*, 7(1), 63–70. (In Indonesian). <https://doi.org/10.36040/mnemonic.v7i1.6961>
- Pelteret, M., & Ophoff, J. (2016). A review of information privacy and its importance to consumers and organizations. *Informing Science*, 19(1), 277–301. <https://doi.org/10.28945/3573>
- Priliyasi, E. (2023). Perlindungan Data Pribadi Konsumen Dalam Transaksi E-Commerce Menurut Peraturan Perundang-Undangan Di Indonesia (Legal Protection Of Consumer Personal Data In E-Commerce According To Laws Dan Regulations In Indonesia). *Jurnal Rechts Vinding*, 12(2), 261–279. (In Indonesian).
- Priskarini, I. A., Pranoto, & Tejomurti, K. (2019). The Role of The Financial Services Authority in The Legal Protection of Privacy Rights in Connection with Personal Data of Fintech Lending Debtor in Indonesia. *Padjadjaran Jurnal Ilmu Hukum (Journal of Law)*, 6(3), 556–575. <https://doi.org/10.22304/pjih.v6n3.a7>
- Pudjastuti, K. G., & Westra, I. K. (2021). Legalitas Mata Uang Virtual Bitcoin Dalam Transaksi Online Di Indonesia. *Kertha Wicara: Jurnal Ilmu Hukum*, 9(11), 1–10. (In Indonesian).
- Rizko Ramadoni, S., Sukarmi, S., & Nur Widhiyanti, H. (2021). Konvergensi Hukum Penentuan Suku Bunga dalam Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi. *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)*, 9(4), 821–837. (In Indonesian). <https://doi.org/10.24843/jmhu.2020.v09.i04.p11>
- Rohmansyah, D. A., Saputra, K. M., & Sholih, B. (2023). Urgensi Perlindungan Hak Asasi Anak Atas Data Pribadi di Era Digitilisasi Berdasarkan Prinsip Negara Hukum. *AL-MANHAJ: Jurnal Hukum Dan Pranata Sosial Islam*, 5(2), 1099–1110. (In Indonesian).
- Setiawan, R. C., Idayanti, S., & Wildan, M. (2023). Perkembangan Komoditi Digital Dalam Aset Kripto Di Indonesia. *Pancasakti Law Journal*, 1(2), 369–384. (In Indonesian). <https://doi.org/10.24905/plj.v1i2.32>
- Sinaga, E. M. C., & Putri, M. Ch. (2020). Formulasi Legislasi Perlindungan Data Pribadi Dalam Revolusi Industri 4.0. *Rechts Vinding: Media Pembinaan Hukum Nasional*, 9(2), 237–256. (In Indonesian). <https://doi.org/10.33331/rechtsvinding.v9i2.428>
- Sinulingga, D. A. (2022). Legal Certainty of Aggregate Data Utilization in The Design of Personal Data Protection Bill. *Jambura Law Review*, 4(1), 18–37. <https://doi.org/10.33756/jlr.v4i1.11973>
- Soraja, A. (2021). Perlindungan Hukum Atas Hak Privasi Dan Data Pribadi Dalam Perspektif Ham. *Seminar Nasional – Kota Ramah Hak Asasi Manusia*, 1, 20–32. (In Indonesian).
- Štarchoň, P., & Pikulík, T. (2019). GDPR principles in data protection encourage pseudonymization through most popular and full-personalized devices – mobile phones. *Procedia Computer Science*, 151(2018), 303–312. <https://doi.org/10.1016/j.procs.2019.04.043>
- Suryawijaya, T. W. E. (2023). Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia. *Jurnal Studi Kebijakan Publik*, 2(1), 55–68. (In Indonesian). <https://doi.org/10.21787/jskp.2.2023.55-68>
- Syailendra, M. R., Lie, G., & Sudiro, A. (2024). Personal Data Protection Law in Indonesia: Challenges and Opportunities. *Indonesia Law Review*, 14(2), 56–72.
- Tatar, U., Gokce, Y., & Nussbaum, B. (2020). Law versus technology: Blockchain, GDPR, and tough tradeoffs. *Computer Law and Security Review*, 38, 105454. <https://doi.org/10.1016/j.clsr.2020.105454>
- Tirtakoesoemah, A. J., & Arafat, M. R. (2019). Penerapan Teori Perlindungan Hukum Terhadap Hak Cipta Atas Penyiaran. *Pena Justisia*, 18(1), 1–14. (In Indonesian). <https://doi.org/10.31941/pj.v18i1.1084>
- Ulya, W., & Pambudi, L. A. (2024). Analisis Kebijakan Cryptocurrency dalam Perspektif Sadd Al-Dzari'ah. *Jurnal Al Azhar Indonesia Seri Ilmu Sosial*, 5(2), 102–111. (In Indonesian).
- Utomo, T. P. (2022). Implementasi Teknologi Blockchain Di Perpustakaan: Peluang, Tantangan Dan Hambatan. *Buletin Perpustakaan*, 4(2), 173–200. (In Indonesian).
- Utomo, Y. A. (2020). Legal Protection for Problem Debtor Related to the Use of the Artificial Intelligence System in Peer to Peer Lending. *Yuridika*, 35(3), 657. <https://doi.org/10.20473/ydk.v35i3.19007>
- Wahyuningtyas, S. Yu. (2024). Legal Issues of Online Reputation Portability in the Digital Economy. *Jurnal Perkotaan*, 15(2), 63–81. <https://doi.org/10.25170/perkotaan.v15i2.5670>
- Yetno, A. (2021). Perlindungan Data Pribadi Dengan Prinsip Mengutamakan Melindungi Privasi Pengguna Dalam Upaya Mewujudkan Tujuan Hukum Di Indonesia. *Satya Dharma: Jurnal Ilmu Hukum*, 4(1). (In Indonesian).

Сведения об авторах



Маюна И Команг Оки – магистрант в области права, факультет права, Университет Бравиджая

Адрес: Индонезия, 65145, провинция Западной Явы, г. Маланг, ул. МТ. Арьоно, д. 169

E-mail: okimayuna04@student.ub.ac.id

ORCID ID: <https://orcid.org/0009-0002-0016-4788>

Google Scholar ID: <https://scholar.google.com/citations?user=H4clKpwAAAAJ>



Девантара Река – доктор права, доцент, факультет права, Университет Бравиджая

Адрес: Индонезия, 65145, провинция Западной Явы, г. Маланг, ул. МТ. Арьоно, д. 169

E-mail: rainerfh@ub.ac.id

ORCID ID: <https://orcid.org/0000-0002-6010-0279>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=58317982600>

Google Scholar ID: <https://scholar.google.co.id/citations?user=kP38YuQAAAAJ>



Руслиджанто Патриция Одри – доктор права, доцент, факультет права, Университет Бравиджая

Адрес: Индонезия, 65145, провинция Западной Явы, г. Маланг, ул. МТ. Арьоно, д. 169

E-mail: patricia@ub.ac.id

ORCID ID: <https://orcid.org/0009-0006-6621-832X>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57201777768>

Google Scholar ID: <https://scholar.google.com/citations?user=TSr2eYoAAAAJ>

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы сообщают 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: 10.19.31 / Право на информацию

Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 21 февраля 2025 г.

Дата одобрения после рецензирования – 15 марта 2025 г.

Дата принятия к опубликованию – 20 июня 2025 г.

Дата онлайн-размещения – 25 июня 2025 г.



Research article

UDC 34:004:346.6:004.7

EDN: <https://elibrary.ru/lqycmn>

DOI: <https://doi.org/10.21202/jdtl.2025.12>

Pseudonymization of Personal Data of Crypto Assets Users: Issues of Legal Regulation in Indonesia

I Komang Oki Mayuna ✉

Brawijaya University, Malang, Indonesia

Reka Dewantara

Brawijaya University, Malang, Indonesia

Patricia Audrey Ruslijanto

Brawijaya University, Malang, Indonesia

Keywords

blockchain technology,
crypto assets,
cryptocurrency,
digital technologies,
law,
legislation,
personal data protection,
personal data,
pseudonymization,
trading in crypto assets

Abstract

Objective: to analyze the possibility of providing legal protection for pseudonymized personal data of crypto assets users in the legal system of Indonesia.

Methods: the work uses a comprehensive legal analysis based on the study of the current regulatory legal acts of Indonesia in the field of personal data protection. The research was carried out using legislative, conceptual and comparative methodological approaches, including an analysis of the Indonesian Law on Personal Data Protection, the EU General Regulation on Personal Data Protection, and the British Data Protection Act.

Results: it was established that pseudonymization of crypto assets user data in Indonesia is feasible from a legal point of view; however, the existing legislation contains significant gaps. The current Indonesian Personal Data Protection Law does not recognize pseudonymized data as a separate category of personal data subject to legal protection. The authors point out the problems with the implementation of the rule for controlling transfers of crypto assets by physical traders. As additional information for the re-identification of pseudonymized data is not stored separately, it increases the risks of privacy violations.

✉ Corresponding author

© Mayuna I K. O., Dewantara R., Ruslijanto P. A., 2025

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0>), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

Scientific novelty: the authors provide a comprehensive analysis of the legal mechanisms for protecting pseudonymized data in the context of cryptocurrency transactions. A conceptual model is proposed for improving national legislation on personal data protection. It implies including pseudonymized data as a separate category of protected information. Recommendations are given, which establish criteria for the legitimate re-identification of pseudonymized data to ensure legal certainty in the field of protecting crypto assets users.

Practical significance: the research results can serve as a theoretical and methodological basis for reforming the Indonesian Law on Personal Data Protection and creating an effective legal mechanism for protecting crypto assets users. The proposed amendments to Article 4 of the said Law will make it possible to include pseudonymized data in the list of protected categories of personal data, which will provide legal certainty for participants in the cryptocurrency market and increase the level of their personal data protection in the digital economy.

For citation

Mayuna, I K. O., Dewantara, R., & Ruslijanto, P. A. (2025). Pseudonymization of Personal Data of Crypto Assets Users: Issues of Legal Regulation in Indonesia. *Journal of Digital Technologies and Law*, 3(2), 275–303. <https://doi.org/10.21202/jdtl.2025.12>

References

- Abdul Karim, M. S., & Hadinata, F. (2023). Implikasi Filosofis Desentralisasi Bitcoin Dalam Perspektif Empire Negri-Hardt. *Jaqfi: Jurnal Aqidah dan Filsafat Islam*, 8(1), 48–60. (In Indonesian). <https://doi.org/10.15575/jaqfi.v8i1.26627>
- Adhiwisaksana, M. F., & Allagan, T. M. P. (2023). Competent Forum and the Applicable Law in Personal Data Protection With Foreign Element. *Indonesian Journal of International Law*, 20(3), 442–470. <https://doi.org/10.17304/ijil.vol20.3.2>
- Alfin, M. H., Idayanti, S., & Rahayu, K. (2024). Regulasi Dan Mekanisme Jual Beli Aset Kripto Di Indonesia. *Jurnal Ilmiah Mahasiswa Ekonomi Syariah (JIMESHA)*, 3(2), 179–188. (In Indonesian). <https://doi.org/10.36908/jimesha.v3i2.312>
- Anand, G., Hernoko, A. Y., & Dharmadji, A. G. (2020). The Urgency of Enacting Personal Data Protection Law As a Patronage From the Development of Communication and Information Technology in Indonesia. *Perspektif*, 25(1), 54–62. <https://doi.org/10.30742/perspektif.v25i1.750>
- Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, 6(1), 132–142. (In Indonesian). <https://doi.org/10.38043/jah.v6i1.4484>
- Asrun, A. M. (2016). Hak Asasi Manusia Dalam Kerangka Negara Hukum: Catatan Perjuangan di Mahkamah Konstitusi. *Jurnal Cita Hukum*, 4(1), 133–154. (In Indonesian). <https://doi.org/10.15408/jch.v4i1.3200>
- Atikah, I. (2023). Perlindungan Hukum Pelanggan Aset Kripto Transaksi Perdagangan Berjangka Komoditi Indonesia. *SALAM: Jurnal Sosial Dan Budaya Syar-I*, 10(2), 497–514. (In Indonesian). <https://doi.org/10.15408/sjsbs.v10i2.31691>
- Ausop, A. Z., & Aulia, E. S. N. (2018). Teknologi Cryptocurrency Bitcoin Untuk Investasi Dan Transaksi Bisnis Menurut Syariat Islam. *Jurnal Sositelknologi*, 17(1), 74–92. (In Indonesian). <https://doi.org/10.5614/sostek.itbj.2018.17.1.8>
- Ayunda, R. (2022). Personal Data Protection to E-Commerce Consumer: What Are the Legal Challenges and Certainties? *Law Reform*, 18(2), 144–163. <https://doi.org/10.14710/lr.v18i2.43307>

- Bolognini, L., & Bistolfi, C. (2017). Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation. *Computer Law and Security Review*, 33(2), 171–181. <https://doi.org/10.1016/j.clsr.2016.11.002>
- Chang, S. E. (2019). Legal Status of Cryptocurrency in Indonesia and Legal Analysis of the Business Activities in Terms of Cryptocurrency. *Brawijaya Law Journal*, 6(1), 76–93. <https://doi.org/10.21776/ub.blj.2019.006.01.06>
- Dat, H. L. N. T., & An, C. T. T. (2024). The Regulation of Data Transmission in the Digital Era: From the European Union's Perspective and Implications for Vietnam. *Vietnamese Journal of Legal Sciences*, 11(2), 1–13. <https://doi.org/10.2478/vjls-2024-0007>
- Dewi, S. (2017). Model Regulation for Data Privacy in the Application of Biometric Smart Card. *Brawijaya Law Journal*, 4(1), 117–128. <https://doi.org/10.21776/ub.blj.2017.004.01.06>
- Faozi, M., & Segara Gustanto, E. (2022). Kripto, Blockchain, Bitcoin, dan Masa Depan Bank Islam: Sebuah Literatur Review. *Quranomic: Jurnal Ekonomi Dan Bisnis Islam*, 1(2), 127–151. (In Indonesian).
- Finck, M., & Pallas, F. (2020). They who must not be identified – distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, 10(1), 11–36. <https://doi.org/10.1093/idpl/ipz026>
- Handoko, R. M., Aulyansyah, B., Trisna, A., & Delon, R. (2024). Implementasi Blockchain Untuk Keamanan Sistem Pembayaran Digital dan Optimalisasi Transaksi Keuangan (Studi Kasus Industri Fintech di Indonesia). *Teknik: Jurnal Ilmu Teknik dan Informatika*, 4(2), 64–74. (In Indonesian).
- Hintze, M., & El Emam, K. (2018). Comparing the benefits of pseudonymisation and anonymisation under the GDPR. *Journal of Data Protection and Privacy*, 2(2), 145–158. <https://doi.org/10.69554/qsst9019>
- Huang, T., & Zheng, S. (2023). Using Differential Privacy to Define Personal, Anonymous, and Pseudonymous Data. *IEEE Access*, 11, 109225–109236. <https://doi.org/10.1109/ACCESS.2023.3321578>
- Imakura, A., Sakurai, T., Okada, Y., Fujii, T., Sakamoto, T., & Abe, H. (2023). Non-readily identifiable data collaboration analysis for multiple datasets including personal information. *Information Fusion*, 98, 101826. <https://doi.org/10.1016/j.inffus.2023.101826>
- Jamwal, S., Cano, J., Lee, G. M., Tran, N. H., & Truong, N. (2024). A survey on Ethereum pseudonymity: Techniques, challenges, and future directions. *Journal of Network and Computer Applications*, 232, 104019. <https://doi.org/10.1016/j.jnca.2024.104019>
- Jati, Hardian Satria, Zulfikar, A. A. (2021). Transaksi Cryptocurrency Perspektif Hukum Ekonomi Syariah. *Al-Adalah: Jurnal Hukum Dan Politik Islam*, 6(2), 137–148. (In Indonesian). EDN: <https://elibrary.ru/mrkhni>. DOI: <https://doi.org/10.35673/ajmpi.v6i2.1616>
- Joo, M. H., & Kwon, H. Y. (2023). Comparison of personal information de-identification policies and laws within the EU, the US, Japan, and South Korea. *Government Information Quarterly*, 40(2), 101805. <https://doi.org/10.1016/j.giq.2023.101805>
- Jose, N. S. (2023). Information and Communication Technologies and the Right to Informational Privacy in Health Care: A Comprehensive Analysis. *Brawijaya Law Journal*, 10(1), 34–58. <https://doi.org/10.21776/ub.blj.2023.010.01.03>
- Kohlmayer, F., Lautenschläger, R., & Prasser, F. (2019). Pseudonymization for research data collection: Is the juice worth the squeeze? *BMC Medical Informatics and Decision Making*, 19(1), 1–7. <https://doi.org/10.1186/s12911-019-0905-x>
- Kumar Rai, B. (2016). Pseudonymization Techniques for Providing Privacy and Security in EHR. *International Journal of Emerging Trends & Technology in Computer Science*, 5(4).
- Limnietis, K. (2021). Cryptography as the means to protect fundamental human rights. *Cryptography*, 5(4), 1–33. <https://doi.org/10.3390/cryptography5040034>
- Maulana, E. T. (2024). Regulasi Travel Rule Terhadap Transaksi Aset Virtual Lintas Batas Dalam Konteks Decentralized Finance Di Indonesia: Studi Banding Terhadap Markets In Crypto-Assets (Mica) Di Uni Eropa. *JURNAL RECTUM: Tinjauan Yuridis Penanganan Tindak Pidana*, 6(3), 565–584. (In Indonesian).
- Mourby, M., Mackey, E., Elliot, M., Gowans, H., Wallace, S. E., Bell, J., Smith, H., Aidinlis, S., & Kaye, J. (2018). Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK. *Computer Law and Security Review*, 34(2), 222–233. <https://doi.org/10.1016/j.clsr.2018.01.002>
- Multazam, M. T., Phahlevi, R. R., Purnomo, M. I., Purwaningsih, S. B., & Sabirov, B. (2024). Securing Blockchain Enterprises: Legal Due Diligence Amidst Rising Cyber Threats. *Padjadjaran Jurnal Ilmu Hukum (Journal of Law)*, 11(1), 26–52. <https://doi.org/10.22304/pjih.v11n1.a2>
- Nanda Sari, A., & Gelar, T. (2024). Blockchain: Teknologi Dan Implementasinya. *Jurnal Mnemonic*, 7(1), 63–70. (In Indonesian). <https://doi.org/10.36040/mnemonic.v7i1.6961>
- Pelteret, M., & Ophoff, J. (2016). A review of information privacy and its importance to consumers and organizations. *Informing Science*, 19(1), 277–301. <https://doi.org/10.28945/3573>

- Priliasari, E. (2023). Perlindungan Data Pribadi Konsumen Dalam Transaksi E-Commerce Menurut Peraturan Perundang-Undangan Di Indonesia (Legal Protection Of Consumer Personal Data In E-Commerce According To Laws Dan Regulations In Indonesia). *Jurnal Rechts Vinding*, 12(2), 261–279. (In Indonesian).
- Priskarini, I. A., Pranoto, & Tejomurti, K. (2019). The Role of The Financial Services Authority in The Legal Protection of Privacy Rights in Connection with Personal Data of Fintech Lending Debtor in Indonesia. *Padjadjaran Jurnal Ilmu Hukum (Journal of Law)*, 6(3), 556–575. <https://doi.org/10.22304/pjih.v6n3.a7>
- Pudjastuti, K. G., & Westra, I. K. (2021). Legalitas Mata Uang Virtual Bitcoin Dalam Transaksi Online Di Indonesia. *Kertha Wicara: Journal Ilmu Hukum*, 9(11), 1–10. (In Indonesian).
- Rizko Ramadoni, S., Sukarmi, S., & Nur Widhiyanti, H. (2021). Konvergensi Hukum Penentuan Suku Bunga dalam Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi. *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)*, 9(4), 821–837. (In Indonesian). <https://doi.org/10.24843/jmhu.2020.v09.i04.p11>
- Rohmansyah, D. A., Saputra, K. M., & Sholih, B. (2023). Urgensi Perlindungan Hak Asasi Anak Atas Data Pribadi di Era Digitilisasi Berdasarkan Prinsip Negara Hukum. *AL-MANHAJ: Jurnal Hukum Dan Pranata Sosial Islam*, 5(2), 1099–1110. (In Indonesian). <https://doi.org/10.37680/almanhaj.v5i2.3054>
- Setiawan, R. C., Idayanti, S., & Wildan, M. (2023). Perkembangan Komoditi Digital Dalam Aset Kripto Di Indonesia. *Pancasakti Law Journal*, 1(2), 369–384. (In Indonesian).
- Sinaga, E. M. C., & Putri, M. Ch. (2020). Formulasi Legislasi Perlindungan Data Pribadi Dalam Revolusi Industri 4.0. *Rechts Vinding: Media Pembinaan Hukum Nasional*, 9(2), 237–256. (In Indonesian). <https://doi.org/10.33331/rechtsvinding.v9i2.428>
- Sinulingga, D. A. (2022). Legal Certainty of Aggregate Data Utilization in The Design of Personal Data Protection Bill. *Jambura Law Review*, 4(1), 18–37. <https://doi.org/10.33756/jlr.v4i1.11973>
- Soraja, A. (2021). Perlindungan Hukum Atas Hak Privasi Dan Data Pribadi Dalam Perspektif Ham. *Seminar Nasional – Kota Ramah Hak Asasi Manusia*, 1, 20–32. (In Indonesian).
- Štarchoň, P., & Pikulík, T. (2019). GDPR principles in data protection encourage pseudonymization through most popular and full-personalized devices – mobile phones. *Procedia Computer Science*, 151(2018), 303–312. <https://doi.org/10.1016/j.procs.2019.04.043>
- Suryawijaya, T. W. E. (2023). Memperkuat Keamanan Data melalui Teknologi Blockchain: Mengeksplorasi Implementasi Sukses dalam Transformasi Digital di Indonesia. *Jurnal Studi Kebijakan Publik*, 2(1), 55–68. (In Indonesian). <https://doi.org/10.21787/jskp.2.2023.55-68>
- Syailendra, M. R., Lie, G., & Sudiro, A. (2024). Personal Data Protection Law in Indonesia: Challenges and Opportunities. *Indonesia Law Review*, 14(2), 56–72.
- Tatar, U., Gokce, Y., & Nussbaum, B. (2020). Law versus technology: Blockchain, GDPR, and tough tradeoffs. *Computer Law and Security Review*, 38, 105454. <https://doi.org/10.1016/j.clsr.2020.105454>
- Tirtakoesoemah, A. J., & Arafat, M. R. (2019). Penerapan Teori Perlindungan Hukum Terhadap Hak Cipta Atas Penyiaran. *Pena Justisia*, 18(1), 1–14. (In Indonesian). <https://doi.org/10.31941/pj.v18i1.1084>
- Ulya, W., & Pambudi, L. A. (2024). Analisis Kebijakan Cryptocurrency dalam Perspektif Sadd Al-Dzari'ah. *Jurnal Al Azhar Indonesia Seri Ilmu Sosial*, 5(2), 102–111. (In Indonesian).
- Utomo, T. P. (2022). Implementasi Teknologi Blockchain Di Perpustakaan: Peluang, Tantangan Dan Hambatan. *Buletin Perpustakaan*, 4(2), 173–200. (In Indonesian).
- Utomo, Y. A. (2020). Legal Protection for Problem Debtor Related to the Use of the Artificial Intelligence System in Peer to Peer Lending. *Yuridika*, 35(3), 657. <https://doi.org/10.20473/ydk.v35i3.19007>
- Wahyuningtyas, S. Yu. (2024). Legal Issues of Online Reputation Portability in the Digital Economy. *Jurnal Perkotaan*, 15(2), 63–81. <https://doi.org/10.25170/perkotaan.v15i2.5670>
- Yetno, A. (2021). Perlindungan Data Pribadi Dengan Prinsip Mengutamakan Melindungi Privasi Pengguna Dalam Upaya Mewujudkan Tujuan Hukum Di Indonesia. *Satya Dharma: Journal Ilmu Hukum*, 4(1). (In Indonesian).

Authors information



Mayuna I Komang Oki – Master of Law Student, Faculty of Law, Brawijaya University
Address: MT. Haryono St 169, Malang City, East Java Province, Indonesia, 65145
E-mail: okimayuna04@student.ub.ac.id
ORCID ID: <https://orcid.org/0009-0002-0016-4788>
Google Scholar ID: <https://scholar.google.com/citations?user=H4clKpwAAAAJ>



Dewantara Reka – Dr. (Law), Associate Professor, Faculty of Law, Brawijaya University
Address: MT. Haryono St 169, Malang City, East Java Province, Indonesia, 65145
E-mail: rainerfh@ub.ac.id
ORCID ID: <https://orcid.org/0000-0002-6010-0279>
Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=58317982600>
Google Scholar ID: <https://scholar.google.co.id/citations?user=kP38YuQAAAAJ>



Ruslijanto Patricia Audrey – Dr. (Law), Associate Professor, Faculty of Law, Brawijaya University
Address: MT. Haryono St 169, Malang City, East Java Province, Indonesia, 65145
E-mail: patricia@ub.ac.id
ORCID ID: <https://orcid.org/0009-0006-6621-832X>
Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57201777768>
Google Scholar ID: <https://scholar.google.com/citations?user=TSr2eYoAAAAJ>

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interest

The authors 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 – February 21, 2025

Date of approval – March 15, 2025

Date of acceptance – June 20, 2025

Date of online placement – June 25, 2025