

© М.Д. Мартынова

Научная статья
УДК 37.013

BIG DATA И КОНТЕКСТЫ КОНФИДЕНЦИАЛЬНОСТИ ДЛЯ ПОДРОСТКОВ В ЦИФРОВОМ ПРОСТРАНСТВЕ

М.Д. Мартынова

Мартынова Марина Дмитриевна,

кандидат философских наук, доцент кафедры философии, Национальный исследовательский Мордовский государственный университет им. Н.П. Огарева, Саранск, Россия.

ORCID: 0000-0003-1244-9721

martynovamd@mail.ru

Аннотация. *Статья посвящена рассмотрению вопросов, касающихся компетентности современных подростков обеспечивать конфиденциальность своих данных в различных контекстах цифровой среды. На основе анализа российских и зарубежных исследований обозначены внутренние и внешние факторы, влияющие на соблюдение / не соблюдение детьми конфиденциальности в межличностном, институциональном и коммерческом контекстах. У подростков размыты границы между публичной и частной сферами в сетевом пространстве, они рассматривают онлайн-среду как удачное место для самовыражения и социальной интеграции. Среди факторов, определяющих отношение школьников к конфиденциальности в Интернете, выделяют уровень медиаграмотности, место проживания, личную мотивацию использования Интернета, ситуативные предпочтения, влияние сверстников, семейные ценности. Сохранение конфиденциальности у подростков обусловлено договоренностями в сообществе, уходом от контроля взрослых, информированием их родителями и педагогами о перечне опасных ситуаций и технических способах поведения в них. В зависимости от контекста подростки прибегают к защите своих данных, руководствуясь одним из принципов: «право на то, чтобы их оставили в покое», «информационное самоопределение в цифровом контексте», «апатия к конфиденциальности». Однако, стремительное развитие технологий, их возрастающая способность агрегировать данные из разных источников, создает ситуацию «запаздывания» образовательных программ и отставания компетенций родителей и педагогов в обучении подростков соблюдению конфиденциальности данных в разных контекстах. Образовательные программы, обучающие информационной безопасности, должны быть сосредоточены на выявлении контекстов и понимании скрытых мотивов людей и компаний, способности анализа динамики опасных ситуаций и способов управления ими, формировании навыков снижения вреда и управления рисками в сети, развитию критического мышления.*

Ключевые слова: *подростки, цифровое пространство, большие данные, межличностный, институциональный и коммерческий контексты, соблюдение конфиденциальности.*

Библиографическая ссылка: Мартынова М.Д. BIG DATA и контексты конфиденциальности для подростков в цифровом пространстве // ЦИТИСЭ. 2024. № 3. С. 398-408.

Благодарности: Исследование выполнено за счет гранта Российского научного фонда № 23-28-01288, <https://rscf.ru/project/23-28-01288/>

Research Full Article

UDK 37.013

BIG DATA AND PRIVACY CONTEXTS FOR TEENAGERS IN THE DIGITAL SPACE

M.D. Martynova

Marina D. Martynova,

Candidate of Philosophy Sciences, Associate Professor of the Philosophy Department, National Research Ogarev Mordovia State University, Saransk, Russian Federation.

ORCID: 0000-0003-1244-9721

martynovamd@mail.ru

Abstract. *The article is devoted to issues related to the competence of teenagers to ensure the confidentiality of their data in various contexts of the digital environment. Based on the analysis of Russian and foreign studies, internal and external factors affecting the observance / non-observance of confidentiality by children in interpersonal, institutional and commercial contexts are identified. Teenagers have blurred the boundaries between the public and private spheres in the digital space, they consider the online environment as a good place for self-expression and social integration. Among the factors determining the schoolchildren attitude to privacy on the Internet, the level of media literacy, place of residence, personal motivation for using the Internet, situational preferences, peer influence, and family values are highlighted. The preservation of confidentiality among adolescents is due to community agreements, avoiding adult control, informing them by parents and teachers about the list of dangerous situations and technical ways of behavior in them. Depending on the context, teenagers resort to protecting their data guided by one of the principles: «the right to be left alone», «information self-determination in a digital context», «apathy towards confidentiality». However, the rapid development of technologies, their increasing ability to aggregate data from different sources creates a situation of «lagging» educational programs and lagging competencies of parents and teachers in teaching adolescents to respect data confidentiality in different contexts. Educational programs for teenagers about information security should focus on identifying contexts and understanding the hidden motives of people and companies, the ability to analyze the dynamics of dangerous situations and how to manage them, the formation of harm reduction and risk management skills in the network, and the development of critical thinking.*

Keywords: *teenagers, digital space, big data, interpersonal, institutional and commercial contexts, confidentiality.*

For citation: *Martynova M.D. BIG DATA and privacy contexts for teenagers in the digital space. CITISE, 2024, no. 3, pp. 398-408.*

Acknowledgments: *the research was carried out at the Russian Science Foundation grant No. 23-28-01288, <https://rscf.ru/project/23-28-01288/>*

Современные школьники являются тем поколением, которое с рождения живет в смешанной реальности¹ (термин введен П. Милгрэм и Ф. Кишино в 1994 г.) и будет работать в профессиональной среде, где ключевыми инструментами будут цифровые технологии. Смешанная реальность имеет сферы, которые складываются стихийно, и сферы, которые структурированы на основе определенных правил и норм. И так же, как в социуме человек с раннего детства должен понимать правила и нормы, обеспечивающие безопасность его жизни, так же и в цифровой среде это исключительно актуально. Со стремительным расширением пространства цифровых технологий эта необходимость возрастает.

Информационная безопасность и цифровая безопасность (в данном случае используем эти категории как синонимичные)², стали предметом экономической и образовательной политики многих стран. Задача по формированию культуры информационной безопасности у детей и школьников общеобразовательных организаций является одной из ключевых по направлению «Информационная безопасность» в программе «Цифровая экономика Российской Федерации»³. Столь пристальное внимание государства к информационной безопасности школьников не случайно, поскольку, по сведениям Росстата, уже по состоянию на 2020 год 96,4% детей в возрасте от 9 до 18 лет являлись активными пользователями Интернет [1, с.142]. Концепция информационной безопасности детей в РФ определяет эту аудиторию как крайне уязвимую с точки зрения информационной безопасности, вследствие нестабильного эмоционального состояния, низкого уровня критичности восприятия и обработки информационного потока.⁴ Они находятся в группе потенциального риска для негативного воздействия и разнообразных интернет-манипуляций.

Одним из ключевых элементов информационной/цифровой безопасности является компетенция соблюдения конфиденциальности своих данных. Подростки знают о необходимости соблюдать конфиденциальность своих данных, но ведут себя по-разному в разных контекстах там, где ее соблюдение необходимо. Каковы причины такого контекстного подхода подростков? Что является их внутренними ограничителями и внешними условиями соблюдения информационной безопасности? Высокая значимость «правильного» поведения школьников в смешанной реальности определяет *цель нашего исследования* как вычленение контекстных планов соблюдения конфиденциальности своих данных подростками и методов формирования у них компетенции соблюдения конфиденциальности как условия безопасного поведения в цифровой среде, бережливого

¹ Смешанная реальность — это сочетание физического и цифрового миров, обеспечивающее взаимодействие между человеком, компьютером и средой. [Электронный ресурс]. – Режим доступа: <https://learn.microsoft.com/ru-ru/windows/mixed-reality/discover/mixed-reality> (Дата обращения: 01.06. 2024)

² Семантическое сходство и различие словосочетаний «цифровая безопасность» и «информационная безопасность» анализируется в исследовании Бегишев И.Р. Семантический анализ термина «цифровая безопасность» // Юрислингвистика. – 2021. – 20. – 24-38. Автор на основе анализа открытых источников и словарных дефиниций выявил, что «в семантическое поле понятия «цифровая безопасность» включаются сегодня три словосочетания «национальная безопасность», «информационная безопасность» и «компьютерная безопасность», юридически и по смыслу связанные с ним». С. 35.

³ «Цифровая экономика Российской Федерации» Распоряжение от 28 июля 2017 г. №1632. [Электронный ресурс]. – Режим доступа: <http://government.ru/docs/28653/> (Дата обращения: 01.06. 2024)

⁴ Концепция информационной безопасности детей в РФ от 28 апреля 2023 г. № 1105-р [Электронный ресурс]. – Режим доступа: <https://www.garant.ru/products/ipo/prime/doc/406740607/#review> (Дата обращения: 01.06. 2024)

отношения к личным данным в разных контекстах. Проблема осознания необходимости соблюдения конфиденциальности получила более пристальное рассмотрение у зарубежных ученых, в то время как российские исследователи более сосредоточены на комплексном подходе к информационной безопасности и цифровой гигиене [2; 3; 4; 5].

Неожиданные рискованные ситуации для подростков связаны не только с тем, что они оставляют свои данные в социальных сетях и на маркетплейсах. С развитием образовательных технологий подростки оставляют цифровые следы на различных образовательных платформах, предоставляющих дополнительные образовательные услуги. Искусственный интеллект может агрегировать все эти данные и составить цифровой профиль, который с помощью цифровой психометрики позволяет прогнозировать будущее поведение человека. [4]. Онлайн-активность детей подвергается обширному коммерческому наблюдению и интеллектуальному анализу данных для создания индивидуально ориентированного контента. Большое количество данных о детях и подростках накапливают государственные организации – школа и здравоохранение, – которые представляют ценность для самых разных субъектов, будь то сами учащиеся и их преподаватели, специалисты по рекламе, брокеры данных, социологи, политические партии и работодатели. Дополнительными «техническими» участниками этой информационной экосистемы становятся поставщики аналитических услуг, оборудования, образовательного программного обеспечения, ИТ-инфраструктуры и интернет-услуг [6].

Агрегированию и профилированию может подвергаться личная информация из профилей соцсетей (об увлечениях, принадлежности к сообществам, религиозных или политических убеждениях), информация о социально-экономическом положении семьи обучающегося, о поведении как потребителя, детализированная информация о промежуточных результатах обучения и состоянии здоровья с официальных платформ [7]. Доступность этой информации, например, для учителей может нанести значительный ущерб ребенку, став субъективным отрицательным фактором при оценке его знаний. Детализированная информация о промежуточных результатах обучения может привести к значительным и долгосрочным последствиям, например, для развития его карьеры в будущем [7]. Даже зафиксированные достижения могут нанести ущерб, если их использовать, например, для сравнения. Данные об образовании – стенограммы, рекомендательные письма, результаты тестов – все чаще запрашиваются потенциальными работодателями [8; 9, с.13].

Такое разнообразие потенциальных последствий открытости данных редко принимается школьниками во внимание. Многие зависят от уровня их цифровой грамотности и отношения к безопасности в цифровой среде. Непрозрачные методы обработки данных усиливают угрозу конфиденциальности, исходящую от способности медиа-технологий деконтекстуализировать личную информацию [10]. Дополнительным фактором риска, по мнению исследователей, является стремление детей в возрасте 11-16 лет к рискованным онлайн-действиям [11]. В свете вышеперечисленного дети, во-первых, выступают цифровыми гражданами, полноправными субъектами онлайн пространства [12], во-вторых, являются уязвимой аудиторией, нуждающейся в защите их конфиденциальности в интернете⁵. Исследование отношения к конфиденциальности в цифровой среде у подростков и формирования компетенции бережного отношения к своим данным имеет особенности, связанные с характером рисков, с которыми сталкивается эта возрастная группа. Различные контексты использования данных могут содержать как близкие по времени (например, мошенничество), так и отложенные по времени (например, трудоустройство) риски.

⁵ Концепция информационной безопасности детей в РФ от 28 апреля 2023 г. № 1105-р [Электронный ресурс]. – Режим доступа: <https://www.garant.ru/products/ipo/prime/doc/406740607/#review> (Дата обращения: 01.06. 2024)

Формирование компетенции соблюдения конфиденциальности как условия безопасного поведения в цифровой среде, бережливого отношения к личным данным в разных контекстах является важным аспектом информационной безопасности. Есть много факторов, определяющих отношение молодежи к конфиденциальности в Интернете в зависимости от места проживания, уровня медиаграмотности, личной мотивации использования интернета. В Концепции информационной безопасности детей в Российской Федерации отмечается, что детям свойственно размещать в открытом доступе в сети интернет личную и семейную информацию, которая нередко используется им во вред. Несмотря на то, что меняются представления о личной жизни - у нового поколения ярко выражено стремление к «публичности», тем не менее подростки начинают заботиться о конфиденциальности [13]. Изменение поколенческих представлений о неприкосновенности частной жизни [14] подтверждает значимость контекстуального рассмотрения конфиденциальности в зависимости от конкретных социальных, культурных или технических контекстов [15].

Исследователи выделяют межличностный, институциональный и коммерческий контекст понимания детьми конфиденциальности [16]. Межличностная конфиденциальность осуществляется, когда данные генерируются отдельными лицами и передаются известным и неизвестным другим лицам, конфиденциальность институциональных и коммерческих данных генерируется с помощью сбора, агрегирования и профилирования данных [17].

Управление конфиденциальностью коммуникаций зависит от контекста отношений как согласования границ конкретных межличностных отношений [18]. Boyd и Marwick используют понятие «сетевой конфиденциальности» для обозначения публичного характера личных сообщений. Особенности сетевых технологий – постоянство, воспроизводимость, масштабируемость и возможность поиска – размывают границы между публичной и частной сферами, опосредованный характер общения в социальных сетях способствует большему саморазглашению личной информации, чем личное взаимодействие. На решения молодежи о том, какой информацией делиться или утаивать большое влияние оказывает ряд ситуативных предпочтений, например, компромисс между риском и выгодой [14], важность онлайн-самопрезентации и экспериментов с идентичностью [18].

В первую очередь детей интересует межличностный контекст, поскольку они стремятся к самостоятельности принятия решений. Часто именно контекст определяет, воспринимается ли ими информация как частная или нет. Исследователи подчеркивают, что для детей конфиденциальность межличностных отношений (то, что они считают личным по отношению к сверстникам, родителям и незнакомым людям) гораздо более важна, чем то, каким образом обрабатывают их данные государственные и частные субъекты [19].

Являясь общедоступными с технической точки зрения, онлайн-пространства, воспринимаются подростками как среда, обеспечивающая конфиденциальность от родителей [18], он может делать там то, что не сможет говорить или делать дома. Подростки гораздо больше беспокоятся о том, что их родители или учителя узнают что-то о них (большинство профилей в ВК являются закрытыми), нежели незнакомые субъекты, будь то люди или государственные и коммерческие организации осуществляют интеллектуальный анализ их данных [17]. И хотя динамика онлайн-среды может угрожать конфиденциальности и потенциально нарушать ее, дети воспринимают ее возможности как поддержку своей идентичности, потребности в самовыражении и поддержки личных отношений и отношений в сообществе, расширяя свой выбор и контроль над личной информацией и, следовательно, свою конфиденциальность в Интернете. Тем самым восприятие подростков и практика защиты частной жизни отличаются от представлений взрослых (родители, педагоги, политики). Отмечено, что подростки наряду с рациональным пониманием конфиденциальности и ее последствий выражают и эмоциональное отношение к ней, они

дают ей следующие определения «осознание себя в сети», «эмоциональные последствия использования интернета» [20].

Соблюдение конфиденциальности у подростков зависит от складывающихся отношений с другими акторами, которые демонстрируют прозрачность, взаимность и вызывают доверие — это школы, органы здравоохранения, правоохранительные органы, потенциальные работодатели и, даже, маркетплейсы. Конфиденциальность воспринимается как социальная ценность, не связанная с использованием технологических манипуляций. Доверие к государственным структурам у подростков и их родителей высоко, и они не задумываются о том, как их персональные данные собираются, обрабатываются и используются, они не думают о долгосрочных последствиях контроля персональных данных детей [19]. В свою очередь, школы и преподаватели не вполне готовы гарантировать прозрачность процессов оперирования данными детей [21].

Тематический анализ поведения детей, проведенный Srivastava S., Wilska T.A., Nyrhinen J., показывает, что дети используют следующие практики: (i) контроль информации, которой делятся сознательно, (ii) контроль информации, предоставленной специально для коммерческого профилирования, (iii) множественные способы использования уведомлений о файлах cookie и (iv) сознательное управление алгоритмами [22]. Для защиты своей частной жизни от злоумышленников дети могут покинуть конкретный веб-сайт или обратиться за помощью к родителям, чего не происходит в отношении коммерческих структур, которые тоже собирают данные [23]. Многие исследования подтверждают, что детям, как и их родителям не хватает общих знаний как о явных, так и о неявных методах сбора данных. Для защиты частной жизни своих детей, родители чаще всего используют либо ограничения, либо посредничество, но оказываются в своем большинстве не осведомлены о способах неявного сбора данных. Такой уровень управления конфиденциальностью с разными акторами информационного пространства определяют как «информационную асимметрию» [19], позволяющую безнаказанно манипулировать данными в сети.

Разница понимания ценности конфиденциальности данных у взрослых и детей отражает межпоколенческий конфликт эпохи цифровых технологий. Поколение «отцов» стремится привить свои ценности «правильного» и «достойного» поведения, руководствуясь соображениями безопасности, поколение «детей» традиционно сопротивляется «старым» нормам. Они не озабочены необходимостью сохранения информации от рекламодателей или платформ социальных сетей [16], часто сопротивляются, считая, что взрослые преувеличивают риски, и не меняют свое поведение в отношении конфиденциальности [17]. Благодаря родителям и учителям в представлении детей хорошо усвоен штамп «stranger danger» (опасный незнакомец) [16]. Например, требование «не разглашайте личную информацию», как правило, укрепляет впечатление о том, что приоритетной опасностью являются незнакомцы. Но оно вступает в противоречие с форматом сетевых отношений со сверстниками, что провоцирует на пренебрежительное отношение к советам взрослых.

Можно выделить три контекстных отношения подростков к защите своих данных: «право на то, чтобы их оставили в покое», «осуществление информационного самоопределения в цифровом контексте», «апатия к конфиденциальности». Позиция «право на то, чтобы тебя оставили в покое», как право на защиту личной информации [24], актуальна в случае использования личной информации об успеваемости ученика для прогнозирования его будущей учебы или трудоустройства. Хотя немало случаев, когда у детей изменяется отношение к учебе в более старшем возрасте. Информационное самоопределение подростка в цифровом пространстве рассматривается ими как неотъемлемое право на автономию личности, выражающееся в праве на свободное выражение мнения, создание произвольного онлайн образа, вступление в онлайн-

сообщества, самостоятельное осуществление покупок [17]. «Апатия к конфиденциальности» [25] возникает из-за ряда причин, среди которых доверие государственным структурам, недостаточный уровень цифровой грамотности, ставшая рутиной необходимость подписывать соглашение о передаче данных, безразличие к передаче своих данным коммерческим структурам, а также отсутствие навыка постоянного контроля над личными данными. Подростки хорошо осведомлены о важности соблюдения конфиденциальности как защиты от кибербуллинга, сексуальных домогательств, общения с незнакомыми людьми в результате обучения в школе кибербезопасности (физиологически-пространственная конфиденциальность – термин Keen). Но в ряде случаев, например, в отношении коммерческих структур, которые имеют большие возможности индивидуального управления данными [17; 26], ни родители, ни подростки, не беспокоятся о раскрытии данных, поскольку не рассматривают целевую рекламу как угрозу их информационной конфиденциальности и возможности нанесения им вреда.

Для повышения устойчивости к коммуникационным рискам образовательная политика практически всех стран опирается на правовое регулирование, пресекающее распространение рискованной информации в интернет, разнообразный инструментарий, обеспечивающий информационную безопасность, взаимодействие с родителями и т.п. Принципиальное значение имеют навыки самостоятельного и критического мышления, позволяющие ориентироваться в информационной среде. В нашей стране приоритетным проектом «Современная цифровая образовательная среда в Российской Федерации» от 25 октября 2016 года № 9⁶ цифровая грамотность школьников обозначена как один из образовательных результатов, а формирование навыков безопасного поведения в цифровой среде и соблюдения конфиденциальности данных является предметом образовательных программ средней школы.

Исследования сформированности у молодежи навыков безопасного использования цифровых технологий показывают противоречивые результаты. Наряду с пониманием того, что цифровая среда является источником разнообразных рисков, тем не менее молодежь достаточно беспечно относится к рекомендациям, пренебрежение которыми делает их уязвимыми. [2]. Беспечное отношение школьников и их родителей к использованию и хранению персональных данных, неосторожное обращение с личной информацией в Интернете свидетельствуют о серьезном расхождении между обеспокоенностью о сохранении конфиденциальности и реальными действиями пользователей в Интернете [3]. Возможными причинами такого разрыва обозначаются наличие доверия к социальной сети, недостаток интернет-грамотности, а также получение определенной выгоды от раскрытия персональной информации [27]. Дети уделяют большое внимание конфиденциальности межличностных отношений в сетевых контекстах, договариваются между собой об обмене или утаивании личной информации, что позволяет им обеспечивать принадлежность к определенному сообществу.

Повышение уровня грамотности детей в области данных и конфиденциальности само по себе является сложной медиаобразовательной задачей [21], способствующей пониманию статуса субъектов данных и цифровых граждан. Дискуссии исследователей о стратегиях защиты детей и подростков от различных форм онлайн-вреда свидетельствуют, что технические навыки использования различных видов защит – пароли или блокирующее программное обеспечение - не являются ключевыми стратегиями [12]. Они создают ложное чувство безопасности. Образование должно быть сосредоточено на контексте рисков, формировании навыков снижения вреда и управления рисками в сети. Навык выявления

⁶ Приоритетный проект «Современная цифровая образовательная среда в Российской Федерации» от 25 октября 2016 года № 9. [Электронный ресурс]. – Режим доступа: <http://government.ru/projects/selection/643/25682/> (Дата обращения: 01.06. 2024)

контекстов – государственные учреждения, образовательные платформы, маркетплейсы, мошенники, сексуальные насильники, хулиганы, опасные для жизни онлайн сообщества, цифровые маркетологи – и понимания скрытых мотивов компаний или людей будет стимулировать развитие критического мышления. Образовательные программы, ориентированные на интернет-опасности, должны уделять приоритетное внимание обучению распознавания динамики опасных ситуаций и способам управления ими, а не только техническим правилам и приемам сохранения конфиденциальности. Избегать манипуляций — значит понимать скрытые мотивы людей или компаний, а не просто удалять файлы cookie или знать, как работает отслеживание.

Таким образом, понимание конфиденциальности у подростков определяется целым рядом факторов. Навыки отношения к личным данным зависят не только от уровня медиаграмотности, но и от социальных, культурных и технологических контекстов. Например, в межличностном контексте подростки более осведомлены о рисках, связанных с общением с незнакомцами, а в институциональном – доверяют школам и медицинским учреждениям, не задумываясь о возможно вредных последствиях использования их данных этими структурами. Исследования показывают, что подростки проявляют разные формы поведения в отношении конфиденциальности, включая «информационное самоопределение», «апатию к конфиденциальности» и утверждение «права на то, чтобы их оставили в покое». Этот контекст показывает, насколько сложно подросткам иногда учитывать последствия своих действий в цифровом пространстве, тем более что они преимущественно воспринимают онлайн-среду как привлекательное место для самовыражения и социальной интеграции.

Отношение подростков к конфиденциальности формируется под воздействием различных факторов, включая влияние сверстников, семейные ценности и образовательные программы. Например, большинство подростков понимает необходимость хранения своих личных данных в безопасности, однако часто пренебрегают этими нормами, упрощая задачу самовыражения в социальных сетях. Для эффективного формирования компетенции соблюдения конфиденциальности у подростков необходимо применять практические методы обучения, сделав акцент на критическом мышлении, анализе рисков, а также на том, как можно предугадать многие ситуации в цифровой среде.

Список источников:

1. Россия в цифрах. 2020: Росстат. 2020. - 550 с. [Электронный ресурс]. – Режим доступа: https://rosstat.gov.ru/storage/mediabank/GOyirKPV/Rus_2020.pdf (Дата обращения: 10.07. 2024)
2. Руденкин Д.В. Уровень развития навыков цифровой гигиены современной российской молодежи: итоги социологического исследования // Социодинамика. 2022. № 1. С. 36-55. DOI: [10.25136/2409-7144.2022.1.37487](https://doi.org/10.25136/2409-7144.2022.1.37487)
3. Пронкина Е.С. Парадокс приватности: почему пользователи социальных медиа раскрывают персональную информацию в публичном пространстве // Вестник РГГУ. Серия «История. Филология. Культурология. Востоковедение». 2018. № 8 (41). С. 155–165. URL: <https://www.elibrary.ru/ypwxpv>
4. Мурзина Ю.С., Позняков В.П. Цифровое поведение и личностные особенности интернет-пользователей // Институт психологии Российской академии наук. Социальная и экономическая психология. 2018. Т. 3, № 3 (11). С. 6–21. URL: <https://www.elibrary.ru/vagofi>
5. Глухов А.П. Цифровая грамотность поколения z: социально-сетевой ракурс // Вестник Томского государственного университета. Философия. Социология. Политология. 2019. № 52. С. 126-137. URL: <https://www.elibrary.ru/jdbzpg>

6. Fitzgerald B. Tracking of teachers and students in Edmodo. 2017. [Электронный ресурс]. – Режим доступа: <https://archive.funnymonkey.com/2017/trackingof-teachers-and-students-in-edmodo.html> (Дата обращения: 10.07. 2024)
7. Minding the data. Protecting learners' privacy and security. Paris. UNESCO. 2022. 55 p. [Электронный ресурс]. – Режим доступа: <https://teaching.globalfreedomofexpression.columbia.edu/resources/minding-data-protecting-learners-privacy-and-security> (Дата обращения: 10.07. 2024)
8. Fain P. IBM Looks Beyond the College Degree. Inside HigherEd. 2019. [Электронный ресурс]. – Режим доступа: <https://www.insidehighered.com/digitallearning/article/2019/10/29/interview-ibm-official-about-companys-new-collar-push-look> (Дата обращения: 10.07. 2024)
9. Rubel A., Jones K.M.L. Student Privacy in Learning Analytics: An Information Ethics Perspective. // The Information Society. 2014. Vol. 32(2). P. 143-159. DOI: [10.1080/01972243.2016.1130502](https://doi.org/10.1080/01972243.2016.1130502)
10. Matz S., Kosinski M., Stillwell D. [et al.] Psychological targeting as an effective approach to real-life persuasive communication // PNAS. 2017. Vol. 45. P. 276–282. DOI: [10.1073/pnas.1710966114](https://doi.org/10.1073/pnas.1710966114)
11. Livingstone S., Haddon L., Görzig A. Children, risk and safety on the internet: research and policy challenges in comparative perspective. - Bristol: Policy Press, 2012. - 11 p.
12. Finkelhor D., Jones L., Mitchell K. Teaching privacy: A flawed strategy for children's online safety // Child Abuse & Neglect. 2021. Vol. 117. 105064. DOI: [10.1016/j.chiabu.2021.105064](https://doi.org/10.1016/j.chiabu.2021.105064)
13. Солдатова Г.У., Олькина О.И. Отношение к приватности и защита персональных данных: вопросы безопасности российских детей и подростков // Национальный психологический журнал. 2015. № 3(19). С. 56–66. URL: <https://www.elibrary.ru/xabvny>
14. Steijn W.M.P., Schouten A.P., Vedder A.H. Why concern regarding privacy differs: The influence of age and (non-)participation on Facebook // Cyberpsychology: Journal of Psychosocial Research on Cyberspace. 2016. Vol. 10(1). 3. DOI: [10.5817/CP2016-1-3](https://doi.org/10.5817/CP2016-1-3)
15. Nissenbaum H. Privacy in Context: Technology, Policy, and the Integrity of Social Life. - Stanford: Stanford Law Books. 2009. - 281 p.
16. Livingstone S., Stoilova M., Nandagiri R. Children's data and privacy online: growing up in a digital age: an evidence review. - London, UK.: London School of Economics and Political Science, Department of Media and Communications, 2019.
17. Keen C. Apathy, convenience or irrelevance? Identifying conceptual barriers to safeguarding children's data privacy // New Media & Society. 2022. Vol. 24(1). P. 50–69. DOI: [10.1177/1461444820960068](https://doi.org/10.1177/1461444820960068)
18. Boyd D., Marwick A.E. Social privacy in networked publics: Teens' attitudes, practices, and strategies. // A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society. - Oxford, UK, 2011. - 1-29 p.
19. Milkaite I., De Wolf R., Lievens E. [et al.] Children's reflections on privacy and the protection of their personal data: A child-centric approach to data protection information formats // Children and Youth Services Review. 2021. Vol. 129. DOI: [10.1016/j.childyouth.2021.106170](https://doi.org/10.1016/j.childyouth.2021.106170)
20. Vespoli G., Taddei B., Imbimbo E. [et al.] The concept of privacy in the digital world according to teenagers // Journal of Public Health. 2024. DOI: [10.1007/s10389-024-02242-x](https://doi.org/10.1007/s10389-024-02242-x)
21. Stoilova M., Livingstone S., Nandagiri R. Digital by Default: Children's Capacity to Understand and Manage Online // Media and Communication. 2020/ Vol. 8. Issue 4. P. 197–207. DOI: [10.17645/mac.v8i4.3407](https://doi.org/10.17645/mac.v8i4.3407)

22. Srivastava S., Wilska T.-A., Nyrhinen J. Children as social actors negotiating their privacy in the digital commercial context // *Childhood*. 2023. Vol. 30(3). P. 235–252. DOI: [10.1177/0907568223118648](https://doi.org/10.1177/0907568223118648)
23. Desimpelaere L., Hudders L., Van de Sompel D. Children’s and parents’ perceptions of online commercial data practices: A qualitative study // *Media and Communication*. 2020. Vol. 8. Issue 4. P. 163–174. DOI: [10.17645/mac.v8i4.3232](https://doi.org/10.17645/mac.v8i4.3232)
24. Müller V.C. Ethics of Artificial Intelligence and Robotics. Stanford Encyclopedia of Philosophy. 2020. [Электронный ресурс]. – Режим доступа: <https://plato.stanford.edu/entries/ethics-ai/> (Дата обращения: 10.07. 2024)
25. Hargittai E., Marwick A. ‘What can I really do?’ Explaining the privacy paradox with online apathy // *International Journal of Communication*. 2016. Vol. 10. P. 3737–3757.
26. Zuboff S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. - London: Profile Books. 2019. - 704 p.
27. Park Y.J. Digital Literacy and Privacy Behavior Online // *Communication Research*. 2013. Vol. 40 (2). P. 215–236. DOI: [10.1177/0093650211418338](https://doi.org/10.1177/0093650211418338)

References:

1. *Russia in numbers: 2020*. Available at: https://rosstat.gov.ru/storage/mediabank/GOyirKPV/Rus_2020.pdf (accessed 10 June 2024)
2. Rudenkin D.V. The level of development of digital hygiene skills of modern Russian youth: the results of a sociological study. *Sociodynamics*, 2022, no. 1, pp. 36-55. (In Russian). DOI: [10.25136/2409-7144.2022.1.37487](https://doi.org/10.25136/2409-7144.2022.1.37487)
3. Pronkina ES. The privacy paradox: why users of social media disclose personal information in public space. *RGGU Bulletin. “History. Philology. Cultural Studies. Oriental Studies”*, 2018, no. 8, pp. 155-65. (In Russian). URL: <https://www.elibrary.ru/ypwpxpv>
4. Murzina Yu.S., Poznyakov V P. Studies of relationship between digital behavior and personal characteristics of internet users. *Institute of Psychology of Russian Academy of Sciences. Social and economic psychology*, 2018, vol. 3, no. 3 (11), pp. 6-21. (In Russian). URL: <https://www.elibrary.ru/vagofi>
5. Glukhov A. P. Generation z’s digital literacy: a social network view // *Tomsk State University Journal of Philosophy, Sociology and Political Science*. 2019, vol. 52, pp. 126–137. URL: <https://www.elibrary.ru/jdbzpg>
6. Fitzgerald B. *Tracking of teachers and students in Edmodo*. 2017. Available at: <https://archive.funnymonkey.com/2017/trackingof-teachers-and-students-in-edmodo.html> (accessed 10 June 2024)
7. *Minding the data. Protecting learners’ privacy and security*. Paris. UNESCO. 2022. 55 p. Available at: <https://teaching.globalfreedomofexpression.columbia.edu/resources/minding-data-protecting-learners-privacy-and-security> (accessed 10 June 2024)
8. Fain P. *IBM Looks Beyond the College Degree*. Inside Higher Ed. 2019. Available at: <https://www.insidehighered.com/digitallearning/article/2019/10/29/interview-ibm-official-about-companys-new-collar-push-look> (accessed 10 June 2024)
9. Rubel A., Jones K.M.L. Student Privacy in Learning Analytics: An Information Ethics Perspective. *The Information Society*, 2014, vol. 32(2), pp. 143-159. DOI: [10.1080/01972243.2016.1130502](https://doi.org/10.1080/01972243.2016.1130502)
10. Matz S., Kosinski M., Stillwell D. et al. Psychological framing as an effective approach to real-life persuasive communication. *PNAS*, 2017, vol. 45, pp. 276–282. DOI: [10.1073/pnas.1710966114](https://doi.org/10.1073/pnas.1710966114)
11. Livingstone S., Haddon L., Görzig A. *Children, risk and safety on the internet: research and policy challenges in comparative perspective*. Bristol, Policy Press Publ., 2012. 11 p.

12. Finkelhor D., Jones L., Mitchell K. Teaching privacy: A flawed strategy for children's online safety. *Child Abuse & Neglect*, 2021, vol. 117, 105064. DOI: [10.1016/j.chiabu.2021.105064](https://doi.org/10.1016/j.chiabu.2021.105064)
13. Soldatova G.U., Olkina O.I. Attitude to privacy and protection of personal data: safety of Russian children and adolescents. *National Psychological Journal*, 2015, vol. 10(3), pp. 56–66. (In Russian). URL: <https://www.elibrary.ru/xabvvnv>
14. Steijn W.M.P., Schouten A.P., Vedder A.H. Why concern regarding privacy differs: The influence of age and (non-)participation on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 2016, vol. 10(1), 3. DOI: [10.5817/CP2016-1-3](https://doi.org/10.5817/CP2016-1-3)
15. Nissenbaum H. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, Stanford Law Books Publ., 2009. 281 p.
16. Livingstone S., Stoilova M., Nandagiri R. *Children's data and privacy online: growing up in a digital age: an evidence review*. London, UK. London School of Economics and Political Science, Department of Media and Communications Publ., 2019.
17. Keen C. Apathy, convenience or irrelevance? Identifying conceptual barriers to safeguarding children's data privacy. *New Media & Society*, 2022, vol. 24(1), pp. 50–69. DOI: [10.1177/1461444820960068](https://doi.org/10.1177/1461444820960068)
18. Boyd D., Marwick A.E. Social privacy in networked publics: Teens' attitudes, practices, and strategies. Proc. "A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society". Oxford, UK. 2011. 1-29.
19. Milkaite I., De Wolf R., Lievens E. et al. Children's reflections on privacy and the protection of their personal data: A child-centric approach to data protection information formats. *Children and Youth Services Review*, 2021, vol. 129. DOI: [10.1016/j.chilyouth.2021.106170](https://doi.org/10.1016/j.chilyouth.2021.106170)
20. Vespoli G., Taddei B., Imbimbo E. et al. The concept of privacy in the digital world according to teenagers. *Journal of Public Health*. 2024. DOI: [10.1007/s10389-024-02242-x](https://doi.org/10.1007/s10389-024-02242-x)
21. Stoilova M., Livingstone S., Nandagiri R. Digital by Default: Children's Capacity to Understand and Manage Online. *Media and Communication*, 2020, vol. 8, issue 4, pp. 197–207. DOI: [10.17645/mac.v8i4.3407](https://doi.org/10.17645/mac.v8i4.3407)
22. Srivastava S., Wilska T.-A., Nyrhinen J. Children as social actors negotiating their privacy in the digital commercial context. *Childhood*, 2023, vol. 30(3), pp. 235–252. DOI: [10.1177/0907568223118648](https://doi.org/10.1177/0907568223118648)
23. Desimpelaere L., Hudders L., Van de Sompel D. Children's and parents' perceptions of online commercial data practices: A qualitative study. *Media and Communication*, 2020, vol. 8, issue 4, pp. 163–174. DOI: [10.17645/mac.v8i4.3232](https://doi.org/10.17645/mac.v8i4.3232)
24. Müller V.C. *Ethics of Artificial Intelligence and Robotics*. Stanford Encyclopedia of Philosophy. 2020. Available at: <https://plato.stanford.edu/entries/ethics-ai/> (accessed 10 June 2024)
25. Hargittai E., Marwick A. 'What can I really do?' Explaining the privacy paradox with online apathy. *International Journal of Communication*, 2016, vol. 10, pp.3737–3757.
26. Zuboff S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London, Profile Books Publ., 2019. 704 p.
27. Park Y.J. Digital Literacy and Privacy Behavior Online. *Communication Research*. 2013, vol. 40 (2), pp. 215–236. DOI: [10.1177/0093650211418338](https://doi.org/10.1177/0093650211418338)

Submitted: 13 August 2024

Accepted: 13 September 2024

Published: 14 September 2024

