Table of Contents

1. Основы неприкосновенности частной жизни 2
1.1. Общие положения 2
1.2. Неприкосновенность частной жизни и конфиденциальность 3
1.3 Неприкосновенность частной жизни в сфере образования 3
1.4. Основания для сбора информации 4
2. Основные определения и нормативно-правовая база в сфере неприкосновенности частной жизни 4
2.1. Неприкосновенность частной жизни в Европейском Союзе 4
2.2. Неприкосновенность частной жизни и персональные данные в России 7
2.3. Виды персональных данных 8
2.3.1 Персональные данные в школе 9
2.4. Процесс обработки и согласие на обработку 11
2.5. Нарушение законодательства об обработке персональных данных 16
2.6. Обзор законодательства в сфере защиты персональных данных в разных странах 19
2.6.1. Бельгия 19
2.6.2. Литва 20
2.6.3. Польша 20
2.6.4. Албания 21
2.6.5. Беларусь 22
2.7. Исключения из законодательства о защите персональных данных 23
2.8. Средства правовой защиты и санкции 23
3. Принципы неприкосновенности частной жизни в сфере образования 25
3.1. Личные дела студентов 25
3.1.1. Информация 25
3.1.2. Недопущение дискриминации 26
3.1.3. Принцип окончательности 26
3.1.4. Успеваемость 26
3.1.5. Хранение и удаление данных 27
3.2. Школьная жизнь 27
3.2.1. Биометрические данные 27
3.2.2. Системы видеонаблюдения 27
3.2.3. Фотографии детей 27
3.2.4. Школьная статистика и прочие исследования 28
4. Информационная открытость и доступ к информации в сфере образования 28
4.1. Определение и различные интерпретации информационной открытости 28
4.2. Правовые основы информационной открытости 29
4.3. Понятие доступа к информации 30
4.4. Информационная открытость в образовании 30
4.4.1. Требования к обеспечению информационной открытости в российских школах 31
4.4.2. Международные требования к уровню информационной открытости веб-сайта 32

4.4.2.1. Описание планируемых результатов обучения 33
4.4.2.2. Программа аттестации 33
4.4.2.3. Оценочные ресурсы 33
4.4.2.4. Мероприятия в рамках текущей аттестации 33
4.4.2.5. Факты, подтверждающие освоение программы обучения 33
4.4.2.6. Использование доказательств освоения учебной программы 33

НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ И ЗАЩИТА ДАННЫХ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ

ИНФОРМАЦИОННАЯ ОТКРЫТОСТЬ И ДОСТУП К ИНФОРМАЦИИ В СФЕРЕ ОБРАЗОВАНИЯ

1. Основы неприкосновенности частной жизни

1.1. Общие положения

В кембриджском словаре английского языка (Cambridge English Dictionary)*неприкосновенность частной жизни (privacy)* в общем смысле определяется как право человека сохранять в тайне аспекты, касающиеся личной жизни и взаимоотношений с другими людьми[1]. Интернет-словарь *Dictionary.com* дает следующее определение понятию *"неприкосновенность частной жизни" (privacy)*: право на защиту от распространения дискредитирующей информации, пристального внимания общественности, тайного наблюдения и несанкционированного разглашения персональных данных или сведений со стороны правительства, компаний, обществ, корпораций или частных лиц[2]". В словаре английского языка "Американское наследие" *неприкосновенность частной жизни (privacy)* рассматривается как состояние, в котором человек чувствует себя свободным от общественного внимания или несанкционированного вторжения в личную жизнь[3]. Согласно словарю английского языка *Merriam Webster Dictionary, неприкосновенность частной жизни (privacy)* - это свобода от неправомерного вторжения в частную жизнь[4].

С юридической точки зрения, неприкосновенность частной жизни - это право, гарантирующее свободу от несанкционированного тайного наблюдения и защиту персональных данных. Таким образом, нормативно-правовые акты, охраняющие

[1] http://dictionary.cambridge.org/dictionary/english/privacy?fallbackFrom=british-grammar
[2] http://www.dictionary.com/browse/privacy?s=t
[3] http://www.yourdictionary.com/privacy#americanheritage
[4] https://www.merriam-webster.com/dictionary/privacy

неприкосновенность частной жизни, могут включать любые требования и предписания, гарантирующие защиту любого лица от посягательств на частную жизнь и недопущение сбора информации, имеющей отношение к данному лицу[5].

Понятие неприкосновенности частной жизни может включать в себя четыре категории: (1) физическая - ограничение, при котором одному лицу запрещается оказывать какое-либо воздействие на другое лицо или сложившиеся обстоятельства. (2) Прецедентная - ограничение, применяемое в отношении четко определенного субъекта. (3) Информационная - недопущение поиска неизвестной информации. (4) Диспозиционная - пресечение попыток получения информации о намерениях и образе мышления определенного лица[6].

1.2. Неприкосновенность частной жизни и конфиденциальность

Важно различать понятия неприкосновенности частной жизни и конфиденциальности. **Конфиденциальность является обязательством**, часто ассоциируемым с такими профессиями как **учителя**, юристы и врачи, и заключается в обязанности последних защищать и хранить в строгой тайне любого рода сведения, относящиеся к лицу, выступающему в качестве субъекта их профессиональных отношений.[7]В некоторых случаях конфиденциальная информация может быть раскрыта, однако круг обстоятельств, позволяющих это сделать, ограничен.

С учетом вышесказанного, неприкосновенность частной жизни, напротив, представляет собой **право (свободу)** хранить в тайне определенные аспекты своей частной жизни.

1.3 Неприкосновенность частной жизни в сфере образования

Неприкосновенность частной жизни в сфере образования базируется на соответствующем законодательстве и практике применения права на неприкосновенность частной жизни в рамках образовательной системы. Наиболее проблемной областью в связи с неприкосновенностью частной жизни в образовательной среде является защита персональных данных учащихся как в школе, так и за ее пределами. Многие ученые дискутируют на тему соблюдения права учащихся - в частности, несовершеннолетних - на неприкосновенность частной жизни, а также на тему эффективного управления данными учащихся в эпоху мгновенного доступа к информации и ее распространения.

Примером соблюдения права на неприкосновенность частной жизни в сфере образования может служить запрет доступа к личным делам учащихся для любых лиц кроме самих учеников, а также их учителей, родителей или законных представителей[8].

Ожидания обучающихся от права на неприкосновенность частной жизни заключаются в наличии возможности отказа от предоставления персональных данных учителям в рамках традиционного школьного контекста. Вопрос неприкосновенности частной жизни в школьной среде вызывает множество споров[9].

---

[5] http://thelawdictionary.org/privacy/
[6] Там же.
[7] Kathryn Dalziel, Privacy in schools: A guide to the Privacy Act for principals, teachers, and boards of trustees. Lithoprint Ltd., Wellington, 2010. c. 7.
[8] Ср. Owasso Independent School Dist. No. I-011 v. Falvo 534 U.S. 426 (2002)
[9] По этому вопросу см. *Scott-Hayward, Christine S. and Fradella, Henry F. and Fischer, Ryan G., Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age (2015). American Journal of*

1.4. Основания для сбора информации

Для того, чтобы вести эффективную деятельность и предоставлять обучающимся необходимые меры поддержки в процессе обучения, образовательному учреждению необходимо собирать персональные данные обучающихся. Персональные данные обрабатываются в силу ряда причин, однако любые подобные данные должны собираться и храниться в соответствии с требованиями закона.

Основными причинами, по которым образовательное учреждение обрабатывает персональные данные обучающихся, могут быть следующими[10]:

- Медицинское обслуживание, т.е. наблюдение за состояние здоровья учащегося с целью избежания несчастных случаев;
- Управление финансами, т.е. контроль внесения оплаты за обучение, предоставление стипендий;
- Безопасность и профилактика/раскрытие преступлений - например, использование систем видеонаблюдения, подготовка отчетов о случаях нарушения безопасности;
- Услуги библиотеки - например, выдача и ведение читательских билетов и карточек, взыскание штрафов;
- Выдача студенческих билетов, зачетных книжек, пропусков, абонементов, удостоверений и т.д.
- Предоставление и техническое обслуживание вычислительных средств и оборудования, включая адреса электронной почты и доступ к сети Интернет;
- Организация и осуществление образовательной деятельности, например, зачисление, контроль успеваемости, составление расписания, определение и оглашение оценок, предоставление рекомендаций;
- Размещение - предоставление и распределение среди студентов жилого фонда, находящегося в собственности образовательного учреждения
- Консультационные услуги, например, консультирование по вопросам профессиональной деятельности и профессиональная ориентация.

2. Основные определения и нормативно-правовая база в сфере неприкосновенности частной жизни

2.1. Неприкосновенность частной жизни в Европейском Союзе

Согласно законодательству Европейского Союза, право на неприкосновенность частной жизни и право на защиту персональных данных являются фундаментальными правами человека. *Хартия Европейского союза по правам человека* (Хартия, 2009) признает право на неприкосновенность частной жизни и право на защиту персональных данных в статьях 7 и 8, соответственно.

В статье 7 Хартии говорится, что "каждый человек имеет право на уважение своей частной и семейной жизни, своего жилья и своих коммуникаций[11]".

Criminal Law, Vol. 43, 2015 and *Daniel R. Dinger, Johnny Saw My Test Score, So I'm Suing My Teacher: Falvo v. Owasso Independent School District, Peer Grading, and a Student's Right to Privacy Under the Family Education Rights and Privacy Act, 30 J.L. & EDUC. 575 (2001).*

[10] Материал частично взят из http://www.bristol.ac.uk/applicants/media/policy-documents/2017/undergraduate/personal-data.pdf с дополнениями, внесенными авторами модуля.

[11] Хартия Европейского Союза по правам человека, OJ C 326, 26.10.2012, с. 391–407

Подобно Хартии, *Конвенция о защите прав человека и основных свобод* (Конвенция, 1950) устанавливает, что "каждый имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции". Важно, что "не допускается вмешательство со стороны публичных властей в осуществление этого права, за исключением случая, когда такое вмешательство предусмотрено законом и необходимо в демократическом обществе в интересах национальной безопасности, общественного порядка" и т.д[12].

Одним из ключевых элементов в рамках понятия "неприкосновенность частной жизни" являются персональные данные. Статья 8(1) Хартии и статья 16(1) *Договора о функционировании Европейского Союза* (ДФЕС) указывают на то, что "каждый человек имеет право на охрану касающихся его сведений личного характера[13]". Помимо прочего, в Хартии закрепляется принцип о том, что "сведения должны использоваться в соответствии с установленными правилами в определенных целях и на основании разрешения заинтересованного лица либо на иных правомерных основаниях, предусмотренных законом". В документе признается право каждого человека на получение доступа к собранным в отношении него данным, и право на устранение в них ошибок. Соблюдение вышеназванны правил поручено независимому органу, учреждаемому каждым из государств-участников ЕС[14].

Европейский парламент и Совет Европейского Союза, действуя в рамках стандартной законодательной процедуры, обязуются установить правила, регулирующие защиту граждан в связи с обработкой и свободным перемещением их персональных данных учреждениями, органами и агентствами Европейского Союза, а также государств-участников, при осуществлении деятельности, на которую распространяется законодательство Европейского Союза.

Как следует из статьи 7 Хартии, "право на уважение ... частной ... жизни" в равной степени распространяется на заинтересованность лица в обеспечении защиты его персональных данных (информации) от несанкционированных или неправомерных действий третьих лиц[15]. В связи с этим в ЕС утверждены несколько документов как на надгосударственном, так и на национальном уровнях.

В 1981 году была принята *Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера (Конвенция 108)*. До настоящего момента Конвенция 108 является единственным в сфере защиты данных международным документом, имеющим обязательную юридическую силу.

Конвенция 108 распространяется на любые процессы обработки данных как в частном, так и в государственном секторе и охватывает, в том числе, данные, обрабатываемые судебными и правоохранительными органами. Конвенция защищает частных лиц от нарушений, которыми может сопровождаться процесс сбора и обработки персональных

[12] Конвенция о защите прав человека и основных свобод с изменениями, внесенными Протоколами № 11 и № 14. Рим, 04.11.1950.

[13] Консолидированные версии Договора о Европейском Союзе и Договора о функционировании Европейского Союза - Консолидированная версия Договора о функционировании Европейского Союза - Протоколы - Приложения - Декларации, являющиеся приложениями к Заключительному договору Межправительственной конференции, утвердившей Лиссабонский договор, подписанный 13 декабря 2007 года - Таблицы эквивалентности. Official Journal C 326 , 26/10/2012 с. 0001 - 0390

[14] Хартия Европейского Союза по правам человека, OJ C 326, 26.10.2012, с. 391–407

[15] Там же.

данных, и стремится упорядочить систему трансграничной передачи персональных данных. Что касается сбора и обработки персональных данных, изложенные в Конвенции принципы касаются прежде всего обеспечения справедливого и правомерного сбора и автоматической обработки данных, которые подлежат хранению для целей, не противоречащих закону, и не могут использоваться не по назначению или храниться дольше предусмотренного срока[16].

Помимо предоставления гарантий в отношении сбора и обработки персональных данных, Конвенция объявляет незаконной обработку специальных данных, таких как: информация о расе, политических и религиозных убеждениях, состоянии здоровья, интимной жизни, имевшихся ранее судимостях и уголовном прошлом, - в том случае если отсутствует возможность обеспечения надлежащих мер безопасности[17].

Конвенция также закрепляет право любого лица знать о том, что в отношении него собирается определенная информация, которую можно корректировать при наличии необходимости и по желанию этого лица. Ограничение прав, предоставляемых Конвенцией, возможно только том случае, когда под угрозой находятся такие первоочередные интересы как, например, национальная безопасность или оборона[18].

В 2018 году в силу вступил Общий регламент Европейского Союза по защите персональных данных, пришедший на смену Регламенту 2016/679 Европейского парламента и Совета Европейского Союза. Вслед за утратившим силу регламентом, а также действующей Директивой 2016/680 новый документ определяет *персональные данные* как любую информацию, относящуюся к поддающемуся идентификации физическому лицу (субъекту персональных данных)[19, 20]. Поддающееся идентификации физическое лицо - это лицо, которое может быть идентифицировано прямым или косвенным путем, в частности на основании таких признаков как имя, идентификационный номер, данные о местоположении, учетная запись в сети Интернет, а также посредством выявления одной или нескольких физических, физиологических, генетических, умственных, экономических, культурных или социальных характеристик, присущих данному физическому лицу.

Общий регламент Европейского Союза по защите персональных данных является актом первичного права, регулирующим процедуру защиты персональных данных граждан ЕС со стороны компаний[21]. Общий регламент призван стать универсальным документом в сфере защиты персональных данных, действующим во всех

[16] Совет Европы, Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера, 28 января 1981 года, ETS 108, режим доступа: http://www.refworld.org/docid/3dde1005a.html

[17] Там же.

[18] Там же.

[19] Регламент ЕС 2016/679 Европейского парламента и Совета Европейского Союза от 27 апреля 2016 года "О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных", объявляющий недействительным Директиву 95/46/ЕС (Директива о защите персональных данных). OJ L 119, 4.5.2016, с. 1–88

[20] Директива (ЕС) 2016/680 Европейского Парламента и Совета Европейского Союза от 27 апреля 2016 года "О защите физических лиц в отношении обработки персональных данных уполномоченными органами с целью предотвращения, расследования, обнаружения и судебного преследования преступлений и применения уголовных наказаний, а также о свободном перемещении таких данных", объявляющая недействительной Рамочное решение Совета ЕС 2008/977/JHA.

[21] Общий регламент Европейского Союза по защите персональных данных вступил в силу 25 мая 2018 года. Полный текст доступен по ссылке: https://gdpr-info.eu/

государствах-участниках ЕС. Таким образом, отдельным государствам больше не придется издавать собственные законы о защите персональных данных, поскольку законодательство в этой области будет унифицировано[22].

Что касается школ, в новом Общем регламенте радикальным образом пересматриваются многие правила, касающиеся обеспечения безопасности персональных данных, поскольку дети приобретают статус "уязвимых граждан", которым требуется "особая защита"[23].

2.2. Неприкосновенность частной жизни и персональные данные в России

В российском законодательстве существует понятие, синонимичное по значению с европейским термином *privacy*. В статьях 23 и 24 *Конституции Российской Федерации* утверждается право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени[24]. Согласно Конституции, государство не имеет права вмешиваться в частную жизнь гражданина и обязуется гарантировать каждому защиту от подобного вторжения со стороны третьих лиц[25].

С точки зрения законодательства, неприкосновенность частной жизни включает в себя как физическую, так и духовную свободу гражданина от внешнего вмешательства в его частную жизнь, которой он вправе распоряжаться по своему усмотрению. Таким образом, неприкосновенными должны оставаться семейные и бытовые аспекты жизни гражданина, в частности круг его друзей и знакомых, его отношение к религии, его не связанная с профессиональной деятельность, увлечения, а также иные отношения, которые гражданин желает сохранять в тайне, в тех случаях, когда это не противоречит закону.

Право на неприкосновенность частной жизни закреплено в нескольких российских законах, принятых за период с 2006 года. В первую очередь, следует подчеркнуть, что регулирование отношений в сфере неприкосновенности частной жизни является прерогативой федерального законодательства, что означает, что региональные и муниципальные органы исполнительной и законодательной власти, а также отдельные учреждения, могут устанавливать собственные нормы и правила в отношении неприкосновенности частной жизни, которые, однако, не могут противоречить федеральному законодательству.

На данном основании в Российской Федерации действует Федеральный закон № 149-ФЗ "Об информации, информационных технологиях и о защите информации"[26], в котором впервые в качестве фундаментального правового принципа провозглашается неприкосновенность частной жизни. Кроме того, существует Федеральный закон № 152-ФЗ "О защите персональных данных", который в общем смысле запрещает обработку персональных данных без предварительного согласия субъекта

---

[22] Подробная информация по ссылке: https://digitalguardian.com/blog/what-gdpr- general-data-protection-regulation-understanding-and-complying-gdpr-data-protection

[23] По этому вопросу см. https://gdpr-info.eu/

[24] "Конституция Российской Федерации" (принята всенародным голосованием 12.12.1993), Гл. 2, ст. 23-24. http://www.constitution.ru/

[25] Там же.

[26] Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации". http://base.garant.ru/12148555/

персональных данных[27]. Перечисленные положения подкрепляются статьей 152.2. *Гражданского кодекса Российской Федерации*, которая вводит ограничение на сбор, хранение, распространение и использование любой информации о частной жизни гражданина, в частности сведений о его происхождении, о месте его пребывания или жительства, о личной и семейной жизни, если иное прямо не предусмотрено законом[28].

Точное определение понятию частной жизни дано в одном из решений Конституционного Суда Российской Федерации, в котором последний указывает на то, что право на неприкосновенность частной жизни включает возможность осуществлять контроль над информацией о гражданине и препятствовать разглашению персональных данных. Помимо этого, Суд постановляет, что понятие частной жизни должно включать в себя личную деятельность, имеющую отношение исключительно к данному лицу, не подлежащую контролю со стороны государства и общества и не противоречащую закону[29].

Российские законодатели предлагают понимать под *информацией* любые данные (факты, сведения и т.д.) вне зависимости от способа и формата их представления. Российское законодательство, кроме того, уделяет внимание процессу раскрытия информации, различая *предоставление* (действия, направленные на получение/передачу информации от/в адрес определенного лица или группы лиц) и распространение (действия, направленные на получение/передачу информации от/в адрес неопределенного лица или неограниченной группы лиц)[30].

2.3. Виды персональных данных

Общий регламент Европейского Союза по защите персональных данных выделяет следующие виды персональных данных:

а) Генетические данные, т.е. любые персональные данные, имеющие отношение к врожденным или приобретенным генетическим характеристикам физического лица и содержащие уникальные сведения о физиологии или состоянии здоровья данного лица, которые могут быть получены на основании проведения анализа биологического образца, взятого у соответствующего физического лица[31].

б) биометрические данные, т.е. получаемые в ходе проведения специальной технической процедуры персональные данные, относящиеся к физическим, физиологическим или поведенческим особенностям лица и позволяющие осуществить идентификацию данного лица, например, посредством изображений лица или дактилоскопических сведений[32].

---

[27] Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных". http://base.garant.ru/12148555/

[28] Гражданский кодекс Российской Федерации (Часть I, II, III и IV) (с изменениями и дополнениями). Принят Государственной Думой 21 октября 1994 года. http://ivo.garant.ru/#/document/10164072/paragraph/44878456:6

[29] Решение Конституционного Суда Российской Федерации от 09.06.2005 N 248-О. http://base.garant.ru/1354478/

[30] Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных", ст. 3. http://base.garant.ru/12148555/

[31] Регламент ЕС 2016/679 Европейского парламента и Совета Европейского Союза от 27 апреля 2016 года "О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных", объявляющий недействительной Директиву 95/46/ЕС (Общий регламент Европейского Союза по защите персональных данных). OJ L 119, 4.5.2016, ст. 4, п. 13.

[32] Там же, п. 14.

в) данные о состоянии здоровья, представляющие собой персональные данные о физическом или психическом здоровье физического лица, включая данные о предоставлении ему медицинской помощи, раскрывающие сведения о текущем состоянии здоровья лица[33].

2.3.1 Персональные данные в школе

Несмотря на то, что право на неприкосновенность частной жизни детей закреплено в нескольких международно-правовых документах, отдельные нормы, направленные на защиту персональных данных, относящихся к детям отсутствовали как в Директиве о защите персональных данных, так и в отдельной Директиве об электронных средствах связи[34]. Как следствие, Общий регламент Европейского Союза по защите персональных данных постановляет, что дети заслуживают дополнительной защиты в отношении их персональных данных, поскольку могут быть не в достаточной степени осведомлены о своих правах, связанных с обработкой персональных данных, о рисках при обращении с персональными данными, последствиях их утраты и способах защиты. Меры дополнительной защиты должны, в частности, применяться по отношению к использованию персональных данных детей в целях маркетинга, создания личностных и пользовательских профилей, а также в случаях сбора относящихся к детям персональных данных с использованием услуг, направленных непосредственно на детей. Кроме того, в отношении детей применяются основополагающие принципы, содержащиеся в Общем регламенте Европейского Союза по защите персональных данных, а именно: добросовестность, пропорциональность и целесообразность. Только те персональные данные детей, которые соответствуют целям обработки с точки зрения объема и содержания могут собираться и обрабатываться. Согласно общему правилу, операторы персональных данных должны принимать в расчет обстоятельства в отношении каждого ребенка и действовать исключительно в интересах последнего. Помимо вышесказанного, персональные данные детей должны быть точными и оперативными. Неточные или неполные данные подлежат удалению или корректировке. Что касается согласия субъекта, законной считается обработка персональных данных ребенка, в случае достижения им 16-летнего возраста. В отношении детей младше 16 лет обработка персональных данных признается законной только при наличии согласия родителя или законного представителя. Государства-участники ЕС имеют право законодательно закрепить более ранний возраст для предоставления согласия, однако он не должен быть менее 13 лет. Говоря о праве доступа к персональным данным, оно может осуществляться как самим ребенком, так и его законным представителем. Персональные данные детей не могут быть использованы в целях, отличных от тех, для которых был организован их сбор.

С учетом перечисленных выше видов персональных данных, предусмотренных законодательством, образовательное учреждение может обрабатывать, помимо прочего, следующие данные[35]:

---

[33] Там же, п. 15.

[34] Директива 2002/58/ЕС Европейского парламента и Совета Европейского Союза от 12 июля 2002 года "Об обработке персональных данных и защите неприкосновенности частной жизни при использовании электронных средств связи (Директива о неприкосновенности частной жизни и электронных средствах связи), OJ L 201, 31.7.2002, с. 37–47

[35] Материал взят из http://www.bristol.ac.uk/applicants/media/policy-documents/2017/ undergraduate/personal-data.pdf с дополнениями, внесенными авторами модуля.

- личные данные (имя, адрес, дата рождения)
- номера телефонов
- адреса электронной почты
- пол
- половая идентичность
- фотографии
- финансовая информация
- школьные оценки
- данные о прохождении аттестации
- личные характеристики
- сведения о поведении и дисциплинарных взысканиях
- сведения об имеющихся судимостях и совершенных правонарушениях
- сведения о состоянии здоровья и наличии ограничений возможностей здоровья
- данные об этнической принадлежности
- сексуальная ориентация
- пищевые потребности
- сведения о религиозных убеждениях
- наличие иждивенцев
- информация об интересах и увлечениях
- любые иные персональные данные, которые на законных основаниях могут использоваться в целях оптимизации процесса обучения.

Сведения об имеющихся судимостях и совершенных правонарушениях, состоянии здоровья, наличии ограничений возможностей здоровья, этнической принадлежности, сексуальной жизни и религиозных убеждениях относятся к категории специальных данных, требующих обеспечения дополнительной защиты и конфиденциальности.

Приведенные выше термины и определения из Общего регламента Европейского Союза по защите персональных находят свое отражение в российском законодательстве почти в полном объеме.

В частности, понятия персональных данных, оператора, обработки, получателя и согласия присутствуют, и их определения близки сформулированным в европейском законодательстве о защите персональных данных. Более того, отдельные нормы российского закона посвящены таким терминам, как "специальные персональные данные", "биометрические персональные данные", а также "трансграничная передача персональных данных".

Образовательное учреждение обязано предпринимать необходимые меры для обеспечения безопасности персональных данных в процессе их обработки. Подобные меры включают в себя, помимо прочего, утверждение локальных регламентов в отношении защиты персональных данных обучающихся.

На основании сравнения множества подобных регламентов, утверждаемых школами по всей стране, можно сделать вывод, что к персональным данным обучающихся относятся, главным образом[36, 37]:

[36] http://ocvvr.com/d/464269/d/polozhenie-o-zaschite-personalnyh-dannyh.pdf

- личное дело обучающегося и табель успеваемости;
- копия свидетельства о рождении;
- информация о членах семьи;
- информация о родителях или законных представителях (опекунах);
- копия паспорта гражданина РФ (в отношении обучающихся старше 14 лет);
- аттестат, подтверждающий получение основного общего образования;
- домашний адрес и телефон;
- фотографии;
- информация о состоянии здоровья и наличии ограничений возможностей здоровья.

К категории данных, которые школа не имеет права собирать и обрабатывать, относятся сведения о личной жизни обучающегося, его политических и религиозных убеждениях.

Справедливым представляется замечание о том, что образовательные учреждения почти никогда не используют генетические данные (за исключением случаев, когда такие данные попадают в категорию данных о состоянии здоровья, и при условии, что последние собираются и обрабатываются образовательным учреждением), в то время как биометрические данные и данные о состоянии здоровья обрабатываются повсеместно: первые в большинстве случаев в целях зачисления и идентификации иностранных студентов, а вторые - в целях предотвращения несчастных случаев, таких как случайные заражения или гибель людей вследствие нераспознанного заболевания.

2.4. Процесс обработки и согласие на обработку

Обработка персональных данных определяется как любая операция или комплекс операций, выполняемых в отношении персональных данных, вне зависимости от использования при этом автоматизированных средств, и включающих в себя сбор, запись, организацию, структурирование, хранение, адаптацию или изменение, извлечение, обращение, использование, раскрытие путем передачи, распространения или любым иным способом, выверку или объединение, ограничение доступа, удаление или уничтожение[38].

Незаконная или недобросовестная обработка влечет за собой соответствующее наказание. Например, одно из образовательных учреждений в Самаре (Россия) осуществляло деятельность, подразумевавшую обработку персональных данных обучающихся. Во ходе проверки было установлено, что на основании приказа директора школы один из работников был назначен ответственным лицом за обработку персональных данных. Однако в действительности обработка данных осуществлялась другим лицом. Таким образом, не уведомив уполномоченный орган об изменениях в процедуре обработки персональных данных, образовательное учреждение допустило нарушение требований, предусмотренных статьей 22 Федерального закона "О

[37] http://cos1601.mskobr.ru/files/pzpd_uchawihsya.pdf

[38] Регламент ЕС 2016/679 Европейского парламента и Совета Европейского Союза от 27 апреля 2016 года "О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных", объявляющий недействительной Директиву 95/46/ЕС (Общий регламент Европейского Союза по защите персональных данных). OJ L 119, 4.5.2016, ст. 4, п. 2.

персональных данных". Впоследствии суд признал образовательное учреждение виновным и назначил наказание в форме предупреждения[39].

Проблема законной и добросовестной обработки персональных данных тесно связана с вопросом согласия, предоставляемого субъектом персональных данных для подтверждения недвусмысленного понимания последним условий обработки и объема обрабатываемых данных.

В соответствии с Общим регламентом Европейского Союза по защите персональных данных, согласие означает любое добровольное, конкретное, информированное и недвусмысленное волеизъявление субъекта персональных данных, на основании которого последний в форме вербального заявления или явного позитивного действия выражает свое согласие на обработку относящихся к нему персональных данных[40].

Европейские законодатели выделяют три элемента согласия, на основании которых оно считается юридически обоснованным, тем самым гарантируя,что субъект действительно согласен на обработку своих персональных данных[41]:

• в момент выражения согласия субъект персональных данных не должен испытывать какого-либо давления извне;

• субъект персональных данных должен иметь полную информацию о цели и последствиях выражения согласия; и

• сфера действия согласия должна быть должным образом ограниченной и конкретной.

Только в случае выполнения всех этих условий согласие будет иметь силу по смыслу законодательства о защите данных.

Очевидно, что прочие требования гражданского законодательства к надлежащим образом выраженному согласию, такие как, например, дееспособность, в равной степени применимы и в сфере защиты данных, поскольку представляют собой фундаментальные юридические предпосылки. Согласие недееспособных лиц является недействительным с юридической точки зрения, поскольку законные основания для обработки персональных данных в отношении данных лиц отсутствуют.

Согласие может выражено быть явным и неявным способом. В первом случае отсутствуют сомнения относительно намерений субъекта; оно может быть как устным, так и письменным. Неявного согласие вытекает из обстоятельств. Любое согласие должны быть выражено в недвусмысленной форме. Это означает отсутствие разумного основания для сомнения в том, что субъект хотел сообщить о своем согласии на обработку относящихся к нему персональных данных. Например, на основании простого бездействия нельзя сделать вывод о предоставлении субъектом недвусмысленного согласия. В случае если речь идет об обработке специальных

[39] https://rospravosudie.com/court-sudebnyj-uchastok-11-samarskoj-oblasti-s/act-238588658/

[40] Регламент ЕС 2016/679 Европейского парламента и Совета Европейского Союза от 27 апреля 2016 года "О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных", объявляющий недействительной Директиву 95/46/ЕС (Общий регламент Европейского Союза по защите персональных данных). OJ L 119, 4.5.2016, ст. 4, п. 11.

[41] Здесь и далее ср. *Handbook on European data protection law*. Агентство Европейского Союза по основным правам, 2014. Совет Европы, 2014, с. 56-60. Режим доступа: http://www.echr.coe.int/Documents/Handbook_data_ protection_ENG.pdf

персональных данных, обязательным условием является явное и недвусмысленное согласие.

Добровольное согласие может быть признано действительным только тогда, когда субъект персональных данных предстает перед реальным выбором, не подвергаясь угрозам и не рискуя быть введенным в заблуждение или испытать серьезные отрицательные последствия, на которые он не давал своего согласия.

Перед принятием решения субъект персональных данных должен обладать достаточной информацией. Решение о том, является ли предоставленная информация достаточной, принимается в каждом конкретном случае. Как правило, информированное согласие представляет собой точное, сформулированное простым языком описание предмета взаимоотношений, требующих выражения согласия, а также последствий предоставления или непредоставления подобного согласия.

Для того чтобы обрести юридическую силу, согласие должно быть конкретным. Это требование обусловлено качеством информации, предоставляемой в отношении предмета согласия. В данном случае значение приобретают обоснованные ожидания рядового субъекта персональных данных. В случае внесения в процедуру обработки персональных данных дополнений или изменений, которые невозможно было предусмотреть в силу объективных причин в момент предоставления согласия, в обязательном порядке необходимо повторное получение согласия от субъекта персональных данных.

Статья 7 Общего регламента Европейского Союза по защите персональных данных предоставляет субъекту право в любое время отозвать свое согласие. Субъект не обязан предоставлять обоснование своего решения об отзыве согласия и не должен опасаться наступления негативных последствий за исключением прекращения действия любых преимуществ и льгот, действовавших в связи с достигнутой ранее договоренностью об использовании персональных данных.

Что касается согласия, российское законодательство устанавливает, что обработка персональных данных может осуществляться только при условии предоставления субъектом персональных данных согласия на обработку последних. Операторы и иные лица, получившие доступ к персональным данным, не имеют права раскрывать их третьим лицам или распространять без предварительного согласия субъекта данных, за исключением предусмотренных законом случаев.

Согласно действующему российскому законодательству, в целях оказания информационной поддержки создаются общедоступные источники персональных данных. В них могут вносится сведения об именах, датах и местах рождения, адресах, номерах телефонов, роде занятий субъектов персональных данных, а также иные данные, полученные исключительно на основании имеющего юридическую силу согласия субъекта. Вышеперечисленные данные подлежат изъятию из общедоступных источников персональных данных в любое время на основании заявления субъекта либо согласно решению суда или иного компетентного государственного органа.

Вслед за положениями европейского законодательства, российский закон требует, чтобы согласие субъекта персональных данных на обработку последних было добровольным, не обусловленным влиянием извне и предоставленным с учетом

интересов самого субъекта. Кроме того, согласие должно быть конкретным, информированным и осознанным. Субъект персональных данных или его представитель могут предоставить согласие на обработку своих персональных данных в любой форме, которая позволяет установить факт предоставления согласия.

Необходимо отметить, что в целях получения любых персональных данных об обучающихся или их родителях российские школы обязаны предоставлять субъектам для заполнения форму согласия на обработку персональных данных, которая служит подтверждением согласия с условиями обработки данных образовательным учреждением (ст. 9 Федерального закона "О персональных данных").

Как и в Общем регламенте Европейского Союза по защите персональных данных, в российском законодательстве в явной форме гарантировано право субъекта персональных данных в любое время отозвать свое согласие[42].

Российское законодательство (равно как и европейское) включает информацию о состоянии здоровья в категорию специальных персональных данных, подчеркивая, что сбор и обработка такой информации запрещены за исключением случаев, когда:

- имеется предварительное письменное согласие субъекта персональных данных;
- подобная информация признается общедоступной самим субъектом персональных данных;
- обработка подобной информации осуществляется в целях защиты жизни, здоровья или иных существенных интересов субъекта персональных данных или других лиц при условии, что получение согласие субъекта является невозможным;
- обработка подобной информации осуществляется в медицинских целях либо в целях постановки диагноза и оказания медицинской помощи при условии, что данные обрабатываются профессиональным медицинским работником, обязанным соблюдать врачебную тайну в соответствии с требованием закона[43].

Примечательно, что статья 41 Федерального закона "Об образовании в Российской Федерации" гарантирует охрану здоровья обучающихся, включая создание особых условий для профилактики заболеваний и оздоровления обучающихся, проведение медицинских осмотров, санитарно-противоэпидемических и профилактических мероприятий, и т.д[44].

Несмотря на это, образовательное учреждение не может получить доступ к информации о состоянии здоровья обучающегося без согласия самого обучающегося или его законного представителя.

Таким образом, данный вопрос регулируется Федеральным законом "Об основах охраны здоровья граждан в Российской Федерации", который предписывает сохранять конфиденциальность информации (сведений), составляющих врачебную тайну, за исключением случаев, когда:

---

[42] Там же, ст. 9.

[43] По этому вопросу см.: там же, ст. 10 и *Handbook on European data protection law*. European Union Agency for Fundamental Rights, 2014. Council of Europe, 2014, с. 87-89. Режим доступа: http://www.echr.coe.int/Documents/Handbook_data_ protection_ENG.pdf

[44] Федеральный закон "Об образовании в Российской Федерации" N 273-ФЗ от 29 декабря 2012 года с изменениями 2019 года, ст. 41. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_140174/

- подобная информация требуется в целях проведения медицинского обследования и лечения гражданина, который в результате своего состояния не способен выразить свою волю;
- существует угроза распространения инфекционных заболеваний, массовых отравлений и поражений;
- информация предоставляется по требованию компетентных органов;
- **медицинская помощь оказывается несовершеннолетнему**[45];
- в ряде других случаев.

В соответствии с действующим законодательством, все образовательные учреждения обязаны разработать собственный внутренний регламент, регулирующий процедуру обработки персональных данных обучающихся[46]. Подобный документ должен включать:

- общие положения;
- определение и объем персональных данных обучающихся и их родителях (законных представителях);
- описание процедуры доступа к персональным данным и и обработки;
- описание способов защиты персональных данных;
- права и обязанности родителей (законных представителей);
- положение об ответственности, предусмотренной за раскрытие персональных данных.

В одном из случаев из правоприменительной практики по данному вопросу Октябрьская средняя школа, расположенная в городе Петухово Курганской области, предоставляла посетителям своего веб-сайта возможность оставить отзыв о деятельности школы. Посетители отправляли сообщение, и в это время веб-сайт собирал персональные данные посетителей (имя и адрес электронной почты). Обработка персональных данных производилась без согласия субъектов данных. Кроме того, на веб-сайте отсутствовал документ, определяющий политику школы в отношении обработки персональных данных. Суд постановил признать юридическое лицо виновным в совершении административного правонарушения и назначил наказание в виде предупреждения[47].

В европейских странах законодательство также обязывает школы разрабатывать подобный внутренний регламент. Например, в Великобритании, школа должна быть готова предоставить документ, подтверждающий добросовестную обработку персональных данных, или уведомление о порядке использования личной информации. Уведомление о порядке использования личной информации необходимо для того, чтобы кратко сформулировать, какие данные собираются и обрабатываются, с какой целью это делается, и каким третьим лицам могут передаваться сведения. Школа обязана получить согласие лица, чьи персональные данные обрабатываются.

---

[45] Федеральный закон "Об основах охраны здоровья граждан в Российской Федерации" от 21.11.2011 N 323-ФЗ (последняя редакция), ст. 13. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_121895/

[46] В качестве примера приводится типовое положение об обработке персональных данных: http://sch1883uz.mskobr.ru/files/ dannie_rabotnikov.pdf

[47] https://rospravosudie.com/court-sudebnyj-uchastok-mirovogo-sudi-19-petuxovskogo-rajona-kurganskoj-oblasti-s/act-238476908/

Уведомление о порядке использования личной информации должно содержать следующую информацию в лаконичной, ясной, понятной и доступной форме:

- идентификационные и контактные данные школы;

- цель и законное основание обработки персональных данных;

- список третьих лиц, которым школа предоставляет персональные данные;

- возможность передачи данных за границы ЕС и способы защиты данных;

- права граждан, например, право подавать жалобы или право отзывать согласие на использование данных.

Документы, отражающие политику в отношении неприкосновенности частной жизни, можно обнаружить на веб-сайтах бельгийских, польских и литовских школ[48, 49]. Поскольку в Белоруссии отсутствует отдельный закон, гарантирующий защиту персональных данных, школы не обязаны утверждать внутренние регламенты (хотя подобные регламенты, в том числе принятые относительно недавно, можно найти на официальных веб-сайтах некоторых частных школ и школ, предоставляющих дополнительные образовательные услуги[50]).

Подводя итог обзору вышеперечисленных определений и понятий, следует отметить, что каждое из них применимо в образовательной среде, поскольку служит для выражения общих представлений о неприкосновенности частной жизни и защите данных, а следовательно, может быть видоизменено таким образом, чтобы отражать специфику образовательного процесса/учреждения в целях защиты прав обучающихся и педагогических работников.

2.5. Нарушение законодательства об обработке персональных данных

В общем и целом данное понятие означает нарушение режима безопасности, повлекшее за собой случайное или противозаконное уничтожение, утрату, изменение, несанкционированное раскрытие или получение доступа к персональным данным в процессе их передачи, хранения или иного процесса обработки[51].

Для того, чтобы продемонстрировать механизм нарушения безопасности данных и способы его устранения в реальных жизненных обстоятельствах, следует ознакомиться с приведенными ниже случаями из правоприменительной практики.

В рамках процесса подачи заявления на зачисление в школу мать одного из будущих первоклассников в явной форме указала в специально предназначенном для этого документе, что она выступает категорически против передачи третьим лицам персональных данных своей дочери, в частности фотографий и телефонных номеров. Осенью проводился ремонт классной комнаты, в связи с чем потребовалась помощь родителей. Некоторые из родителей получили на свои мобильные телефоны текстовые

[48] https://www.isb.be/quick-links/privacy-policy
[49] http://www.nordangliaeducation.com/our-schools/warsaw/privacy-policy
[50] http://robolab.by/assets/files/politika_rb.pdf
[51] Регламент ЕС 2016/679 Европейского парламента и Совета Европейского Союза от 27 апреля 2016 года "О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных", объявляющий недействительной Директиву 95/46/ЕС (Общий регламент Европейского Союза по защите персональных данных). OJ L 119, 4.5.2016, ст. 4, п. 12.

сообщения, отправленные от имени родительского комитета с просьбой о помощи. Мать первоклассника обратилась в прокуратуру Приволжского района города Казани с жалобой на то, что ее телефонный номер был предоставлен третьим лицам без ее согласия. В официальном ответе районного прокурора от 16 января 2017 года указано, что по результатом официальной проверки директору "Гимназии № 40" вынесено представление о привлечении виновных к дисциплинарной ответственности. В отношении учителя начато административное судопроизводство в связи с нарушением процедуры сбора, хранения, использования и распространения персональных данных. Учителю грозит штраф в размере от 500 до 1000 рублей[52].

В ходе проверки, проведенной прокуратурой по другому делу в Карелии, выяснилось, что на официальном интернет-сайте "Лоухской средней общеобразовательной школы" была размещена программа профессионального воспитания, которая помимо общих сведений об учащихся содержала фамилии, имена, отчества обучающихся и их родителей, адреса места жительства, номера телефонов, места работы. Кроме того, были перечислены дети, воспитывающиеся в неполных и малообеспеченных семьях. Также указаны имеющиеся у конкретных школьников хронические заболевания и вредные привычки. Указанные сведения были обнародованы на школьном сайте без получения чьего-либо согласия вопреки требованиям Федерального закона "О персональных данных". В связи с нарушением прав обучающихся и их родителей на неприкосновенность частной жизни, личную и семейную тайну в отношении юридического лица и директора школы прокуратура района возбудила дела об административном правонарушении, предусмотренном статьей 13.11 Кодекса об административных нарушениях Российской Федерации. По результатам рассмотрения дела мировой суд назначил юридическому лицу административное наказание в виде штрафа в размере пяти тысяч рублей, а также оштрафовал директора школы. Незаконно размещенные на школьном сайте персональные данные граждан были удалены[53].

В целях обеспечения соблюдения законодательства о защите персональных данных как внутри, так и за пределами Европейского Союза учреждены специальные органы.

Уполномоченный по защите персональных данных[54], являющийся независимым органом, гарантирует, что Европейская комиссия надлежащим образом применяет законодательство, направленное на защиту персональных данных граждан. Уполномоченный несет ответственность за ведение открытого реестра, фиксирующего все выполняемые Комиссией операции, подразумевающие обработку персональных данных. Помимо прочего, Уполномоченный занимается расследованием случаев нарушения безопасности персональных данных, ведет реестр учета операций по обработке персональных данных департаментами Комиссии и взаимодействует с Европейским инспектором по защите данных.

---

[52] http://www.evening-kazan.ru/articles/skandal-v-kazanskoy-gimnazii-uchitelnicu-nakazali-za-sms-roditelnice.html

[53] http://prokuratura.karelia.ru/struktura/gorodskie-i-rayonnye-prokuratury/prokuratura-loukhskogo-rayona/loukhi_news/page_2784/?forBlind=on

[54] Подробная информация по данному вопросу: https://ec.europa.eu/info/departments/data-protection-officer_en#contact

Европейский инспектор по защите данных[55] представляет собой независимый орган Европейского Союза в области защиты персональных данных. Его миссия заключается в осуществлении контроля и обеспечении безопасности персональных данных и неприкосновенности частной жизни. Он также обязан следить за появлением новых технологий, которые могут снизить эффективность защиты персональных данных, и выступать перед Судом Европейского Союза, предоставляя профессиональные консультации по вопросам толкования законодательства о защите персональных данных. Инспектор взаимодействует с государственными и иными надзорными органами для достижения большей согласованности действий, направленных на защиту персональных данных. Европейский инспектор по защите данных призван осуществлять функции независимого центра передового опыта и компетенций в сфере внедрения и укрепления принятых в ЕС стандартов защиты персональных данных и соблюдения неприкосновенности частной жизни как в теории, так и на практике.

В каждом государстве-участнике существует организация или лицо, исполняющее функции вышестоящего органа по вопросам защиты персональных данных на национальном уровне[56]. К таковым, например, относятся:

- Генеральный инспектор по защите персональных данных (Польша);
- Государственная инспекция по защите персональных данных (Литва);
- Комиссия по защите неприкосновенности частной жизни (Бельгия);

На местном уровне школы обязаны разработать отлаженную процедуру, регулирующую выявление нарушений безопасности данных, предоставление сведений о подобных нарушениях и их расследование. Соответствующие органы должны быть без промедления поставлены в известность о фактах таких нарушений.

Необходимо обеспечивать сохранность персональных данных любыми способами, адекватными природе данных, например:

- использование надежных паролей
- уничтожение бумажных отходов, содержащих конфиденциальную информацию, и окончательное удаление данных с электронных носителей
- шифрование данных на электронных носителях
- установка систем защиты доступа и антивирусного программного обеспечения
- хранение электронных устройств в запертых помещениях
- отключение настроек автоматического заполнения
- проверка поставщиков данных на соответствие необходимым требованиям.

В случае если школа не может обеспечить адекватные меры безопасности, уполномоченный орган должен отреагировать на это соответствующим образом, в частности, он может назначить наказание в виде штрафа.

Подобно европейским странам, многие государства, не входящие в ЕС, учредили органы, занимающиеся вопросами сохранности персональных данных/неприкосновенности частной жизни. В Белоруссии существует два основных органа, деятельность которых направлена на обеспечение защиты персональных

[55] Подробная информация: https://edps.europa.eu/about-edps_en
[56] Подробная информация об органах, осуществляющих защиту персональных данных в разных странах мира: https://www.dlapiperdataprotection.com/ index.html?t=world-map&c=PL&c2=RU

данных: Оперативно-аналитический центр при Президенте Республики Беларусь, а также Министерство связи и информатизации Республики Беларусь. В России существует Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (так называемый Роскомнадзор), ответственность которой в настоящее время распространяется на 402 030 операторов данных[57]. В Албании независимым наблюдательным органом является Агентство по защите персональных данных, учрежденное в соответствии с Главой VIII Закона "О защите персональных данных" и возглавляемое выборным Уполномоченным[58].

2.6. Обзор законодательства в сфере защиты персональных данных в разных странах

2.6.1. Бельгия[59]

Общий регламент Европейского Союза по защите персональных данных находит свое отражение в бельгийском законе "О защите неприкосновенности частной жизни в отношении обработки персональных данных"[60].

Несовершеннолетний, не достигший возраста, в котором появляется способность осознавать свои действия и управлять ими, может выразить согласие на обработку своих персональных данных через законного представителя (статья 1, §8 Закона), который в свою очередь может в любое время отозвать согласие несовершеннолетнего, действуя от его имени.

Не существует определенного возраста, по достижении которого можно установить появление у несовершеннолетних способности осознавать и управлять своими действиями, однако Рекомендация от 16 сентября 2002 года (Рекомендация 38/2002), принятая Комиссией по защите неприкосновенности частной жизни, указывает на то, что несовершеннолетние обычно приобретают способность понимать сущность вещей и явлений в возрасте от 12 до 14 лет.

Кроме того, существует региональный (фламандский) закон "Об открытости (прозрачности) деятельности органов управления" Инстанцией, несущей ответственность за надлежащее исполнение требований закона, является Комиссия по защите частной жизни (Комиссия по защите неприкосновенности частной жизни) и Фламандский надзорный комитет.

Например, в одном из случаев, связанных с защитой неприкосновенности частной жизни, учащемуся фламандской школы по итогам учебного года было выдано свидетельство уровня B (позволяющее перейти в следующий класс, однако предусматривающее некоторые ограничения на этапе выбора траектории обучения). Однако ни сам учащийся, ни его родители не получили отчета, подтверждающего достижение названного результата. Следовательно, они не были проинформированы о возможности опротестовать принятое школой решение. Суд постановил, что представленные по делу факты содержат признаки нарушения Закона о об открытости

[57] Использована информация ресурса: https://rkn.gov.ru/personal-data/register/
[58] Подробная информация: http://www.ceecprivacy.org/main.php?s=2&k=albania
[59] См. https://uk.practicallaw.thomsonreuters.com/2-502-2977?__lrTS=20170413125855005 &transitionType=Default&contextData=(sc.Default)
[60] https://cwisdb.kuleuven.be/pisa/nl/juridisch/privacywet.htm

деятельности органов управления (статья 35), а также нарушения Кодекса среднего образования (статья 115/6, §4, 2°).

2.6.2. Литва

Нормативно-правовую базу в сфере защиты персональных данных составляет закон "О правовой защите персональных данных", отражающий основные требования Общего регламента Европейского Союза по защите персональных данных. В законе излагаются основополагающие принципы защиты персональных данных, определяется процедура их обработки, а также права субъектов. К сожалению, закон не уделяет особого внимания процессу обработки персональных данных несовершеннолетних. Согласно закону, ответственность за осуществление контроля над его исполнением и применением возлагается на Государственную инспекцию по защите персональных данных[61].

2.6.3. Польша[62]

Будучи членом ЕС, Польша воплотила положения общеевропейского законодательства в сфере защиты персональных данных в законе "О защите персональных данных" от 29 августа 1997 года. Данный закон регулирует процедуру обработки персональных данных, определяя их в соответствии с Общим регламентом Европейского Союза по защите персональных данных.

До наступления возраста 18 лет ребенок не обладает полной гражданской дееспособностью, в связи с чем в отношении него действуют следующие нормы:

- Поскольку до достижения 13-летнего возраста ребенок считается недееспособным, любое юридически значимое действие от его имени может быть произведено только родителями или законными представителями (за исключением заключаемых в рамках повседневной деятельности договоров).
- В случае если возраст ребенка составляет от 13 до 18 лет, он самостоятельно может производить юридически значимые действия при наличии согласия родителя(-ей).

Родители являются законными представителями ребенка до тех пор, пока на него распространяются их родительские права. Если родительскими правами в отношении ребенка обладают оба родителя, каждый из них по-отдельности может выступать в качестве законного представителя.

Однако родители должны совместно принимать решения по важным вопросам, касающимся их ребенка. Определение понятия "важные вопросы, касающиеся ребенка" отсутствует. Данное понятие обычно интерпретируется судами как включающее в себя следующие элементы жизни ребенка:

- место проживания (включая место проведения школьных каникул).
- Школа.
- Будущая работа.

---

[61] См. The Summary of Research Studies “Good Practice in Children’s Privacy Protection” and “The Analysis of
Target Groups Needs” in Lithuania and Italy, c.7.

[62] См. https://uk.practicallaw.thomsonreuters.com/6-520-7945?__lrTS=20170413130810421 &transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1

- Медицинское обслуживание.

В одном из рассмотренных судебных дел между истцом и школой возник конфликт на основании имевшегося у истца подозрения о том, что его сын подвергается "физической и эмоциональной травле" в школе, что вынудило истца перевести детей в другую школу. М.П. (истец) направлял директору школы письма с описанием ситуации и требованием сообщить ему о предпринятых школой в отношении спорного вопроса мерах. В результате школа предприняла действия, которые, по мнению директора, должны были привести к выяснению всех обстоятельств и не допустить, чтобы подобные инциденты случались в дальнейшем. Истец утверждал, что на заседаниях совета школы и родительского комитета были зачитаны его письма, комментарии учителей и заключение психолога. Согласно предъявленной жалобе, оба названных школьных органа обсуждали сложившуюся в семье истца ситуацию на основании информации из написанных им писем, однако истец не давал своего разрешения на предание огласке содержания переписки. На основании вышеизложенного истец обратился к Главному инспектору по защите персональных данных с жалобой, в которой требовал удаления персональных данных о его семье в целях восстановления нарушенных прав в соответствии с законом. Инспектор отклонил жалобу М.П., поэтому последний опротестовал решение инспектора в суде первой инстанции. Суд отменил решение апелляционной инстанции, а также предшествующее ему решение.

Суд отметил, что инспектор допустил небрежность в процессе сбора свидетельских показаний, а также принял к рассмотрению неполные по содержанию документы, предоставленные школой. Согласно мнению суда первой инстанции, с учетом предоставления неполных по содержанию документов невозможно было на данной стадии установить, содержались ли в них так называемые специальные данные. Инспектор обратился с апелляцией в суд вышестоящей инстанции, однако последний полностью поддержал решение суда первой инстанции и вынес в адрес Инспектора предписание о пересмотре дела.

2.6.4. Албания

В Албании существует закон " О защите персональных данных" № 9887 от 10.03.2008 (с дополнениями и изменениями). Определение персональных данных в законе совпадает с определением. приведенным в Общем регламенте Европейского Союза по защите персональных данных. В частности, специальные данные обозначают любую информацию о физическом лице, относящуюся к его расовому или этническому происхождению, политическим взглядам, членству в профессиональных союзах, религиозным или философским убеждениям, судимостям и уголовном прошлом, а также подразумевает сведения о состоянии здоровья и сексуальной жизни[63].

Кроме того, право на защиту неприкосновенности частной жизни гарантируется албанской Конституцией и некоторыми другими законами. Несмотря на то, что ни в одном из этих законов дети не выделяются в отдельную категорию, предполагается, что действие законов распространяется на каждого гражданина, а право на неприкосновенность частной жизни относится к фундаментальным правам человека.

[63] The International Comparative Legal Guide to: Data Protection 2016. A practical cross-border insight into data protection law, 3rd edition. Published by Global Legal Group, p. 7. Режим доступа: https://www2.deloitte.com/content/dam/Deloitte/al/Documents/legal/Deloitte-Albania -Legal-Guide-Data-Protection-2106.pdf

Согласно отдельным источникам, существующие законы, защищающие право детей на неприкосновенность частной жизни, фактически не применяются, в результате чего как родители, так и учителя на регулярной основе вторгаются в личную жизнь детей. Поскольку многие факты нарушения этих прав происходят внутри семьи или в школе, дети зачастую не имеют возможности подать жалобу в компетентные органы, так как у них отсутствует доступ к бесплатной юридической помощи. То же самое можно сказать о несоблюдении права детей на неприкосновенность частной жизни в полицейских участках, следственных изоляторах и колониях[64].

В июле 2016 года уполномоченным по защите прав на доступ к информации и охрану персональных данных была проведена проверка на предмет соблюдения региональным департаментом образования округа Эльбасан Закона № 9887 и связанных с ним внутренних нормативно-правовых актов.

В ходе административного расследования было установлено, что в региональном департаменте образования не был разработан документ, регулирующий процедуру защиты персональных данных, и департамент не заключал с учителями соглашений о неразглашении конфиденциальной информации. Персональные данные учителей, например, их идентификационные номера, были опубликованы на портале регионального департамента в сети Интернет[65]. Создаваемые школьными психологами личные дела, содержащие сведения об обучающихся с ограничениями возможностей здоровья, фактах наличия психических заболеваний и проблемного поведения, должны были храниться в течение трех лет после завершения данными детьми обучения в школе, однако не была разработана процедура, в соответствии с которой должны были осуществляться данные мероприятия. Результаты испытаний, которые проходили учителя в рамках профессиональной аттестации, также публиковались на портале регионального департамента образования в сети Интернет. Проанализировав факты, уполномоченный пришел к выводу, что последние составляют административное правонарушение, предусмотренное статьями 27 и 28 Закона "О защите персональных данных". Публикация на веб-сайте департамента уникальных идентификационных номеров учителей, была признана нарушением их права на неприкосновенность частной жизни, поскольку существовала возможность установить личность учителя посредством использования кода, связанного с идентификатором. Уполномоченный пришел к выводу, что выявленные нарушения безопасности персональных данных обучающихся и учителей были серьезными и могли быть квалифицированы как административное правонарушение. Региональный департамент образования был оштрафован на 100 000 албанских леков (примерно 800 Евро) за нарушение требований статей 27 и 28 Закона "О защите персональных данных"[66].

2.6.5. Беларусь[67]

Основным документом Республики Беларусь, регулирующим сбор, хранение и использование персональных данных, является закон "Об информации,

[64] Alternative Report for the situation of children's rights and the implementation of the Convention on the Rights of the Child in Albania prepared by the Children's Human Rights Centre of Albania – CRCA, Tirana, 2004, p. 12. Режим доступа: http://www.crin.org/en/docs/resources/treaties/crc.38/Albania_ngo_report.pdf
[65] www.darelbasan.arsimi.gov.al
[66] Решение 44 Уполномоченного по защите прав на доступ к информации и охрану персональных данных от 29.07.2016, http://www.idp.al/hetimi-administrativvendime/
[67] См. http://www.lexology.com/library/detail.aspx?g=f8279c06-f1f4-45cd-9fe0-52e5fdc904a9

информатизации и защите информации" от 10 ноября 2008 года № 455-З. Персональные данные определены законом как основные (напр., имя, дата рождения и пол) и дополнительные (напр., постановка на налоговый учет, воинская обязанность и сведения об образовании) персональные данные физического лица, подлежащие в соответствии с законодательными актами Республики Беларусь внесению в регистр населения, а также иные данные, позволяющие идентифицировать такое лицо.

2.7. Исключения из законодательства о защите персональных данных[68]

Общий регламент Европейского Союза по защите персональных данных дает право государствам-участникам законодательным путем ограничивать права субъектов персональных данных в силу следующих обстоятельств:

- национальная безопасность, общественная безопасность, оборона страны;
- предотвращение, расследование, обнаружение и судебное преследование преступлений или нарушений, связанных с нарушением этических норм, установленных для регламентированных профессий;
- важные экономические или финансовые интересы ЕС или отдельных государств-участников; и
- защита субъектов персональных данных или прав и свобод других граждан.

Помимо прочего, Директива об электронных средствах связи и защите персональных данных позволяет государствам-участникам ЕС внедрять законодательные меры с целью хранения персональных данных в течение ограниченного времени в силу перечисленных выше причин.

2.8. Средства правовой защиты и санкции

Государства-участники ЕС обязаны обеспечить субъектам персональных данных гарантии восстановления их нарушенных прав. Следовательно, Общий регламент Европейского Союза по защите персональных данных предоставляет субъектам данных следующие права:

- Административные средства защиты при помощи государственного контролирующего органа[69];
- Судебная защита в случае любых нарушений прав, предусмотренных национальным законодательством[70];
- Компенсация оператором ущерба, причиненного в связи с допущенными в процессе обработки персональных данных нарушениями. Однако оператор может быть освобожден от ответственности полностью или частично, в случае если сможет доказать, что нарушение произошло не по его вине[71];

При введении в действие общеевропейского законодательства предполагается, что государства-участники обязаны предусмотреть во внутренних нормативно-правовых актах санкции, применяемые к нарушителям[72].

---

[68] См. https://www.loc.gov/law/help/online-privacy-law/eu.php#_ftn32
[69] Регламент ЕС 2016/679, гл. 8. Режим доступа: https://gdpr-info.eu/chapter-8/
[70] Там же.
[71] Там же.
[72] Там же.

Например, в Албании[73] отсутствует специальное обязательство сообщать о нарушении, однако законодатель предусматривает наказание за несанкционированное раскрытие конфиденциальной информации. Законом предусмотрен штраф в размере от 10 000 до 150 000 албанских леков. Более того, в отдельных случаях, нарушение безопасности конфиденциальной информации может быть уголовно наказуемым деянием, совершение которого влечет за собой лишение свободы на срок до двух лет.

Стоит отметить, что в последние годы албанский Уполномоченный демонстрирует активность, вынося операторам и контроллерам данных различного рода рекомендации и предписания, а также применяя к ним меры административной ответственности, с целью привлечения внимания к правам и обязанностям, вытекающим из положений действующего законодательства.

В Бельгии[74] обработка персональных данных, противоречащая закону "О защите неприкосновенности частной жизни в отношении обработки персональных данных" может быть уголовно наказуемым деянием (статьи 37-39 Закона), влекущим за собой штраф в размере от 550 до 110 000 Евро. Кроме того, суд может вынести решение о конфискации носителя, содержащего персональные данные, безопасность которых была нарушена. Суд может вынести предписание об уничтожении данных либо о запрете контролировать обработку любых персональных данных, напрямую или через посредников, на период до двух лет.

Согласно польскому[75] законодательству, в случае нарушения любого из положений законодательства о защите персональных данных, Главный инспектор может предписать обеспечить соответствие требованиям закона посредством принятия административного решения. Невыполнение подобного решения может привести к наложению штрафа в размере 50 000 Евро. Более того, невыполнение требований закона, может повлечь за собой уголовное наказание. Нарушители отдельных положений закона о защите персональных данных наказываются частичным ограничением свободы, лишением свободы на срок до трех лет или дополнительным штрафом.

В Литве[76] любое нарушение требований закона о защите персональных данных предполагает административную ответственность. Данная ответственность наступает в случае незаконной обработки персональных данных, а также в случае нарушения норм, применяемых к процессу обработки персональных данных и защите неприкосновенности частной жизни по смыслу закона "Об электронных средствах связи". Незаконная обработка данных (напр., противоправное использование адреса электронной почты или иных сведений о лице, вне зависимости от целей такого использования) предполагает наложение штрафа в размере 500-1000 литов (145-290 Евро). За повторное нарушение предусмотрен штраф в размере 1000-2000 литов.

---

[73] The International Comparative Legal Guide to: Data Protection 2016. A practical cross-border insight into data protection law, 3rd edition. Published by Global Legal Group, p. 13. Режим доступа: https://www2.deloitte.com/content/dam/Deloitte/al/Documents/legal/Deloitte-Albania -Legal-Guide-Data-Protection-2106.pdf

[74] См. https://uk.practicallaw.thomsonreuters.com/2-502-2977?__lrTS=20170413125855005 &transitionType=Default&contextData=(sc.Default)

[75] См. https://uk.practicallaw.thomsonreuters.com/6-520-7945?__lrTS=20170413130810421 &transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1

[76] http://www.ebaltics.com/00705594

В России[77] за нарушение законодательства в сфере защиты персональных данных может применяться гражданская (моральный вред), административная (штраф) и уголовная (лишение свободы) ответственность.

Следует отметить, что российские законы, гарантирующие безопасность персональных данных, были значительно усилены в течение последних лет, в связи с чем в Роскомнадзор поступает большое количество обращений. С другой стороны, операторы данных все чаще пытаются опротестовать приказы и решения Роскомнадзора, касающиеся применения к операторам различных санкций и ограничения доступа к Интернет-ресурсам. В результате стремительно развивается правоприменительная практика, связанная с наложением санкций за несоблюдение требований российского законодательства в сфере защиты персональных данных. В ближайшем будущем административные санкции за нарушение безопасности данных могут быть ужесточены путем внесения изменений в действующий закон.

3. Принципы неприкосновенности частной жизни в сфере образования

Рабочая группа по вопросам охраны права на неприкосновенность частной жизни и защиты персональных данных в процессе своей деятельности подготовила ряд заключений, касающихся защиты персональных данных детей. Одно из таких заключений адресовано руководителям школ[78]. В данном заключении обсуждаются вопросы защиты информации, относящейся к детям. Заключение в первую очередь распространяется на тех, кто обрабатывает персональные данные детей. Говоря о школах, к таким лицам относятся учителя и представители школьной администрации. Данный документ предназначен для того, чтобы провести анализ общих принципов защиты персональных данных детей и обосновать значимость их применения в школьном контексте.

Документ различает фундаментальные принципы (по смыслу Общего регламента Европейского Союза по защите персональных данных) и принципы, обусловленные спецификой образовательного процесса, путем помещения фундаментальных принципов в школьный контекст. В целях настоящего модуля представляется целесообразным подробнее рассмотреть вторую группу принципов.

3.1. Личные дела студентов

3.1.1. Информация

В некоторых странах законодательство позволяет школьной администрации с целью формирования личных дел обучающихся предоставлять для заполнения формы, содержащие персональные данные. Подобные формы должны информировать субъектов данных о факте сбора и обработки их персональных данных, о целях такой обработки, о контроллерах данных и о порядке использования прав субъектов на доступ к данным и внесения в них исправлений[79]. Личные дела обучающихся должны содержать только персональные данные, необходимые для осуществления школой

[77] См. https://content.next.westlaw.com/2-502-2227?transitionType=Default&contextData=(sc.Default)&__lrTS=20170516055929769&firstPage=true&bhcp=1

[78] Здесь и далее представлен обзор документа: Article 29 Data Protection Working Party, Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools), 398/09/EN, WP 160 (Feb. 11, 2009), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_en.pdf.

[79] Там же, с. 12

предусмотренных законом действий, и не должны использоваться в иных целях. Не следует собирать данные, в которых нет необходимости.

3.1.2. Недопущение дискриминации

Некоторые данные, содержащиеся в вышеназванных формах, могут послужить причиной для дискриминации, например, данные о расовой принадлежности, статусе иммигранта, наличии ограничений возможностей здоровья. Обычно подобная информация собирается для того, чтобы обеспечить надлежащий уровень осведомленности школы о наличии обучающихся, испытывающих культурные (например, языковые) или экономические трудности, в целях минимизации которых школа может предпринять необходимые действия.

Необходимо предпринимать адекватные меры защиты любой информации, которая может спровоцировать дискриминацию: обработка должна осуществляться в отдельных файлах силами квалифицированных и уполномоченных на выполнение данных функций лиц, обязавшихся исполнять требование о неразглашении профессиональной тайны. Согласие на обработку данных, которые могут послужить причиной для дискриминации, должно быть явным и недвусмысленным[80].

3.1.3. Принцип окончательности

Известны случаи, когда руководство школы, зачастую в маркетинговых целях, передает имена и адреса обучающихся третьим лицам. Подобные действия являются нарушением принципа окончательности, поскольку предназначенные для использования внутри школы данные, применяются в ненадлежащих целях. Согласно Общему регламенту Европейского Союза по защите персональных данных, персональные данные детей не могут использоваться в целях, отличных от тех, которые были указаны в рамках обоснования для их использования. В случае если третьи лица запрашивают персональные данные родителей и/или учеников для использования их в маркетинговых целях, передача этих данных моет быть осуществлена только при условии предварительного уведомления законных представителей и получения их согласия (либо согласия самих детей, в зависимости от степени их дееспособности)[81].

3.1.4. Успеваемость

Существуют страны, в которых существуют устоявшиеся в течение многих лет традиции, касающиеся размещения в открытом доступе отметок об успеваемости. Такая система гарантирует возможность сравнения результатов и облегчает процесс возможного оспаривания и пересмотра результатов. В этих странах школы должны строго соблюдать предусмотренные законом требования и публиковать в минимальном объеме только те персональные данные, которые абсолютно необходимы.

Особый вызов - это размещение результатов успеваемости в сети Интернет, с помощью которой очень удобно доводить до сведения заинтересованных лиц необходимую информацию. Риск, связанный с данным способом коммуникации, предполагает принятие специальных мер безопасности с целью ограничения доступа к персональным данным. Безопасность может быть обеспечена посредством использования защищенного веб-сайта или персональных паролей, выдаваемых законным

[80] Там же.
[81] Там же, с. 13

представителям либо самим детям при условии достижения ими дееспособного возраста[82].

3.1.5. Хранение и удаление данных

В отношении личных дел обучающихся применяется фундаментальный принцип о том, что никакая информация не должна храниться дольше срока, необходимого для достижения цели, ради которой она собиралась. В связи с этим необходимо тщательно следить за тем, какие сведения из личных дел следует хранить в образовательных или профессиональных целях, а какую необходимо удалить (например, сведения о применявшихся в отношении обучающихся дисциплинарных взысканиях или наказаниях)[83].

3.2. Школьная жизнь

Вопросы, связанные с защитой персональных данных, возникают в отношении различных повседневных аспектов школьной жизни. Существует ряд средств отслеживания численности обучающихся в школе, некоторые из которых могут сильнее остальных угрожать неприкосновенности частной жизни.

3.2.1. Биометрические данные

С течением времени в школы все активнее используют системы контроля и управления доступом. Подобные системы могут собирать биометрические данные обучающихся (отпечатки пальцев или ладони, сканирование сетчатки) при входе в школу. В отношении средств сбора биометрических данных следует применять принцип пропорциональности. Настоятельно рекомендуется предусмотреть простой способ, благодаря которому законные представители могли бы выразить отказ от предоставления персональных данных детьми. В случае отказа детям должны быть выданы электронные пропуска или иные средства доступа на территорию школы[84].

3.2.2. Системы видеонаблюдения

В целях обеспечения безопасности в школах все чаще используются системы видеонаблюдения. Не существует универсальных рекомендаций, которые можно в равной степени применить ко всем аспектам школьной жизни во всех школьных помещениях. Способность систем видеонаблюдения в той или иной степени ограничивать права и свободы личности предполагает ответственное планирование мест их установки в школе. Это означает, что видеонаблюдение должно присутствовать только в тех местах, где оно действительно необходимо, и только в том случае, если отсутствует возможность использования средств, в меньшей степени угрожающих неприкосновенности частной жизни. Камеры видеонаблюдения должны устанавливаться в тех местах, где это целесообразно и приемлемо, камер не должно быть слишком много.

3.2.3. Фотографии детей

Зачастую школы поддаются искушению опубликовать (в печатных СМИ или в Интернете) фотографии своих учеников. Особое внимание школы должны уделять размещению фотографий своих учеников в Интернете. Необходимо в каждом случае анализировать, что изображено на фотографии, а также целесообразность и причину ее

[82] Там же, с. 14
[83] Там же, с. 15
[84] Там же.

публикации. Дети и их законные представители должны быть поставлены в известность о факте публикации. Если речь идет о групповых фотографиях, изображающих школьные мероприятия, школы имеют право не обращаться за получением согласия к родителям в тех случаях, когда это не противоречит законодательству и когда фотографии не позволяют с легкостью определить личность отдельного ребенка. Однако в таких случаях школы обязаны информировать детей, родителей и законных представителей о том, что фотографии будут сделаны и о том, как они будут использованы. Таким образом, обучающиеся смогут отказаться от своего присутствия на фотографии[85].

3.2.4. Школьная статистика и прочие исследования

В большинстве случаев для сбора статистики персональные данные не требуются. Однако в исключительных случаях они необходимы, например, для получения сведений о вовлечении выпускников в профессиональную деятельность. Согласно Общему регламенту Европейского Союза по защите персональных данных, результаты статистических исследований не должны повлечь за собой непосредственную или опосредованную идентификацию субъектов персональных данных.

4. Информационная открытость и доступ к информации в сфере образования

4.1. Определение и различные интерпретации информационной открытости

В кембриджском словаре английского языка (Cambridge English Dictionary)**отрытость (transparency)** в общем смысле определяется как свойство, реализуемое в духе открытости и при отсутствии тайн[86]. Согласно словарю английского языка Merriam Webster Dictionary, открытость характеризуется осведомленностью и наличием доступа к информации, в частности в отношении методов ведения бизнеса[87]. Международная некоммерческая организация *Transparency International* (2006) определяет открытость как прозрачность правил и процедур внутри организации с одной стороны и в отношениях между организацией и пользователями ее услуг с другой стороны. Это означает наличие прозрачных процедур, целей и задач в работе учреждения. Кроме того, это означает непреложное право граждан на получение необходимой информации[88].

Понятие открытости противоположно по значению понятию секретности. Секретность означает намеренное или умышленное сокрытие действий, в то время как открытость понимается как инструмент, помогающий довести до сведения общественности важную информацию, как способность граждан принимать участие в принятии политических решений и как ответственность правительства в рамках юридического процесса.

Основными параметрами открытости являются прозрачность, гласность, точность, легкость доступа к информации и участие в принятии решений на различных административных уровнях.

---

[85] Там же.
[86] http://dictionary.cambridge.org/dictionary/english/transparency?fallbackFrom=british-grammar
[87] https://www.merriam-webster.com/dictionary/transparent
[88] По статье: Khaled Serhan, *Administrative Transparency in Public Secondary Schools in Jordan*, European Scientific Journal May 2016 edition vol.12, No.13, с. 158. Режим доступа: http://eujournal.org/index.php/esj/article/viewFile/7467/7192

Все перечисленные параметры не должны противоречить высшему общественному интересу. Таким образом, открытость не требует раскрытия информации, если в результате этого может быть нарушена безопасность государства или отдельных граждан[89].

4.2. Правовые основы информационной открытости

Понятие открытости в европейском законодательстве тесно связано с понятиями неприкосновенности частной жизни и обработки персональных данных. Вступительное положение 39 Регламента 2016/679[90] устанавливает, что любая обработка персональных данных должна быть справедливой и не противоречащей закону. Физические лица должны быть осведомлены о том, что их персональные данные собираются, используются, просматриваются или иным способом обрабатываются, а также о том, в каком объеме это происходит или будет происходить в будущем.

Принцип открытости предполагает, что любые передаваемые или принимаемые сообщения, относящейся к обработке персональных данных, должны быть доступными, понятными и изложенными в простой и ясной форме. Данный принцип в частности касается доступности для субъектов данных информации о личности контроллера и целях обработки, а также любой дополнительной информации, обеспечивающей справедливую и прозрачную обработку данных физических лиц и их право на получение достоверных сведений об обрабатываемых персональных данных.

Физические лица должны быть осведомлены о рисках, требованиях, гарантиях и правах в отношении обработки персональных данных, а также о том, каким образом осуществлять эти права в рамках процесса обработки данных. В частности, особые цели для сбора персональных данных должны быть однозначными, обоснованными и определенными на момент сбора данных.

Кроме того, Регламент провозглашает, что открытость предполагает лаконичность любого адресованного общественности или отдельному субъекту сообщения и, помимо прочего, требует его визуализации в тех случаях, когда это допустимо. Подобные сообщения могут быть доведены до сведения общественности в электронном виде, например, посредством размещения на веб-сайте. Данное положение имеет особую значимость в том случае, когда большое количество заинтересованных лиц и техническая сложность практической реализации осложняют понимание субъектом того, кем и с какой целью собираются его персональные данные, в частности когда речь идет о рекламе в Интернете[91].

Следует отметить, что Регламент учитывает интересы детей, подчеркивая, что последние заслуживают дополнительной защиты. Таким образом, любые адресованные ребенку сообщения должны быть сформулированы простым и доступным языком, чтобы последний имел возможность без труда понять их[92].

---

[89] Там же.

[90] Регламент ЕС 2016/679 Европейского парламента и Совета Европейского Союза от 27 апреля 2016 года "О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных", объявляющий недействительной Директиву 95/46/ЕС (Общий регламент Европейского Союза по защите персональных данных), OJ L 119, 4.5.2016.

[91] Там же, вступительное положение 58.

[92] Там же.

Более того, принципы справедливой и прозрачной обработки данных требуют, чтобы субъект был проинформирован о факте и целях обработки. Контроллер обязан предоставить субъекту данных любую дополнительную информацию необходимую для обеспечения справедливой и прозрачной обработки с учетом особых обстоятельств и условий, в которых обрабатываются персональные данные. Субъект данных должен быть осведомлен о факте осуществления профилирования и его последствиях. В тех случаях, когда происходит сбор данных о субъекте, последний должен быть проинформирован о том, обязан ли он предоставлять свои данные, а также о последствиях отказа от их предоставления. Данная информация может быть представлена в сочетании со стандартными условными графическими символами, чтобы в явной, понятной и доступной форме довести до сведения субъектов краткий, но эффективный обзор целей предстоящей обработки данных[93].

Наконец, согласно требованиям Регламента, в целях увеличения степени открытости следует внедрять механизмы сертификации, а также специальные печати и знаки для защиты персональных данных, позволяющие субъектам оперативно оценить уровень защищенности информации в процессе приобретения соответствующих товаров и услуг[94].

Несмотря на то, что обработка персональных данных должна осуществляться в соответствии с предусмотренными законом целями, основываться на принципах справедливости и открытости и не нарушать права физических лиц, правоохранительные органы имеют право проводить негласные следственные действия и использовать системы видеонаблюдения. Подобные мероприятия могут быть организованы с целью предотвращения, расследования, обнаружения и судебного преследования преступлений и применения уголовных наказаний, включая охрану и минимизацию угроз общественной безопасности, в случае если эти действия не противоречат закону, учитывают законные интересы физических лиц и являются необходимыми и соразмерными в демократическом обществе[95].

4.3. Понятие доступа к информации

В соответствии с изложенными выше положениями, свобода информации является одним из параметров открытости. Свобода информации может обозначать доступ граждан к информации, находящейся в распоряжении органов государственной власти[96].

4.4. Информационная открытость в образовании

Национальный институт оценки результатов обучения (США) под открытостью понимает обеспечение внутренним и сторонним наблюдателям легкого доступа к значимым и доступным для понимания сведениям о результатах обучения и

[93] Там же, вступительное положение 60.
[94] Там же, вступительное положение 100.
[95] Директива (ЕС) 2016/680 Европейского Парламента и Совета Европейского Союза от 27 апреля 2016 года "О защите физических лиц в отношении обработки персональных данных уполномоченными органами с целью предотвращения, расследования, обнаружения и судебного преследования преступлений и применения уголовных наказаний, а также о свободном перемещении таких данных", объявляющая недействительной Рамочное решение Совета ЕС 2008/977/JHA, вступительное положение 26.
[96] Patrick Birkinshaw, *Transparency as a Human Right*, in Christopher Hood and David Heald (Eds.), (2006) *Transparency: The Key to Better Governance?*, Oxford, New York: Oxford University Press, c. 50.

эффективности образовательного учреждения. Сведения являются значимыми и доступными для понимания, когда они контекстуализируются и логическим образом согласуются с целями образовательного учреждения в отношении результатов обучения. К значимым сведениям могут относиться детализированные результаты, сгруппированные в зависимости от специальности, способностей, пола, расы и этнического происхождения и предоставляющие динамический анализ или прогноз, а также сопоставление с общенациональными нормами и показателями аналогичных учреждений[97].

Современное использование понятия "открытость" в российской образовательной практике тяготеет к трем основным моделям:

- *открытость операционная* - доступность образования любому желающему, вне зависимости от его исходных характеристик (возраст, уровень имеющихся знаний), реализуемая, в том числе, через использование дистанционных форм обучения и внесистемных образовательных сервисов; возможность обучения в ритме, удобном учащемуся;
- *открытость институциональная* - ориентация на учет интересов всех участников образовательного процесса; возможность для потребителей образовательных услуг активно участвовать в формировании и развитии системы образования, в оценке качества образовательных услуг и управлении им (в том числе через деятельность коллегиальных органов управления: управляющих советов, общественных советов и др.); учет системой образования внешних социокультурных условий и потребностей современного общества;
- *открытость информационная* - обеспечение двустороннего информационного обмена между различными участниками образовательного процесса и иными заинтересованными субъектами, обеспечивающего удовлетворение потребностей стейкхолдеров в информации о деятельности образовательной системы и позволяющего образовательной организации и/или органу управления образованием получать обратную связь[98].

4.4.1. Требования к обеспечению информационной открытости в российских школах

В дополнение к Федеральному закону Российской Федерации "Об образовании" существует Постановление Правительства Российской Федерации № 582[99], в котором определены объем и содержание сведений, размещаемых в открытом доступе на официальном сайте образовательной организации, с целью обеспечения соответствия Федеральным законам "О персональных данных" и "Об образовании".

Согласно Постановлению, образовательная организация на своем официальном веб-сайте размещает, помимо прочего, следующую информацию:

---

[97] http://www.learningoutcomeassessment.org/TransparencyFrameworkIntro.htm

[98] Мерцалова Т. А. Информационная открытость системы образования: вопросы эффективности государственной политики // Вопросы образования. Москва. - 2015. № 2 С. 40–75. Режим доступа: http://vo.hse.ru/en/

[99] Постановление Правительства Российской Федерации № 582 от 10 июля 2013 г. «Об утверждении правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети "Интернет" и обновления информации об образовательной организации».

а) о дате создания образовательной организации, о месте нахождения образовательной организации и ее филиалов, режиме, графике работы, контактных телефонах и об адресах электронной почты; о структуре и об органах управления образовательной организации, в том числе: фамилии, имена, отчества и должности руководителей структурных подразделений; об уровне образования; о формах обучения; о нормативном сроке обучения; об описании образовательной программы; о календарном учебном графике; о численности обучающихся по реализуемым образовательным программам за счет бюджетных ассигнований и за счет средств физических и (или) юридических лиц; о языках, на которых осуществляется образование; о федеральных государственных образовательных стандартах; о руководителе образовательной организации, его заместителях, в том числе: фамилия, имя, отчество руководителя, его заместителей; должность руководителя, его заместителей; контактные телефоны; адрес электронной почты; о персональном составе педагогических работников с указанием уровня образования, квалификации и опыта работы, в том числе: фамилия, имя, отчество работника; занимаемая должность; преподаваемые дисциплины; ученая степень; ученое звание; данные о повышении квалификации и (или) профессиональной переподготовке (при наличии); о наличии и условиях предоставления обучающимся стипендий, мер социальной поддержки; о трудоустройстве выпускников;

б) копии устава образовательной организации и лицензии на осуществление образовательной деятельности;

в) иную информацию, опубликование которой является обязательным в соответствии с действующим законодательством.

Образовательная организация обязана обновлять вышеперечисленные сведения не позднее 10 рабочих дней после внесения в них изменений.

Следует отметить, что программные средства, которые используются для функционирования официального сайта, должны обеспечивать, помимо прочего, возможность копирования информации на резервный носитель, обеспечивающий ее восстановление, а также защиту информации от уничтожения, модификации, блокирования доступа и иных незаконных или неправомерных действий.

4.4.2. Международные требования к уровню информационной открытости веб-сайта

Национальный институт оценки результатов обучения разработал структуру открытости информации[100] с целью оказания поддержки образовательным учреждениям в процессе обмена критериями, подтверждающими освоение программ очного и дистанционного обучения. Структура основывается на проведенном исследовании контента веб-сайтов образовательных учреждений и выделяет шесть ключевых компонентов оценки результатов обучения. Образовательные организации могут использовать Структуру для того, чтобы проанализировать свои веб-сайты и установить, насколько доступно на них представлены факты, подтверждающие освоение программы обучения, насколько полезными и значимыми являются представленные сведения для целевой аудитории веб-сайта. Каждый раздел Структуры

[100] Transparency Framework. Urbana, IL: University of Illinois and Indiana University, National Institute for Learning Outcomes Assessment (NILOA). Режим доступа: http://www.learningoutcomeassessment.org/TransparencyFrameworkIntro.htm

рассматривает один из компонентов оценки результатов обучения, представляющий потенциальный интерес для определенной аудитории, и предлагает рекомендации, направленные на повышение уровня понимания общественностью сути данного компонента.

Кроме того, в Структуре изложены базовые принципы коммуникации с аудиторией посредством веб-сайта. Например, размещаемые на веб-сайте данные должны быть значимыми и понятными как можно большему числу людей. В целях выстраивания эффективной коммуникации с различными типами аудитории веб-сайт должен предоставлять пользователям возможность оставлять обратную связь в отношении размещенных на нем материалов.

Полностью открытый веб-сайт должен содержать информацию о всех перечисленных ниже компонентах.

4.4.2.1. Описание планируемых результатов обучения

В описании планируемых результатов обучения четко определяются ожидаемые знания, навыки, установки, компетенции и умения, которые студенты должны приобрести в течение периода обучения в учебном заведении.

4.4.2.2. Программа аттестации

В разработанную образовательным учреждением программу сбора фактов, подтверждающих освоение программы обучения, могут входить общеуниверситетские или действующие в рамках определенной программы мероприятия, включающие в себя методы оценки результатов обучения, способы сбора данных, применяемые подходы и сроки выполнения.

4.4.2.3. Оценочные ресурсы

Оценочные ресурсы предполагают наличие необходимой информации, а также проведение для преподавателей и административных работников тренингов, помогающих им понимать, разрабатывать, внедрять, доводить до сведения заинтересованных лиц и применять на практике факты, подтверждающие освоение программы.

4.4.2.4. Мероприятия в рамках текущей аттестации

Мероприятия в рамках текущей аттестации включают в себя информацию о полном объеме выполненных или предстоящих проектов и прочих мероприятий, направленных на определение уровня подготовки обучающихся, доработку материалов или обеспечение соответствия критериям отчетности.

4.4.2.5. Факты, подтверждающие освоение программы обучения

К фактам, подтверждающим освоение программы обучения, относятся результаты прохождения обучающимися аттестационных мероприятий. В данном случае речь может идти о фактах косвенного (напр., опросы), и непосредственного (напр., портфолио) обучения, а также о показателях эффективности образовательного учреждения (напр., процент успешно прошедших аттестацию обучающихся).

4.4.2.6. Использование доказательств освоения учебной программы

Данный компонент дает представление о том, насколько эффективно используются сведения, подтверждающие освоение программы обучения, для того, чтобы за счет изменения политики и повседневной практики образовательного учреждения

определить точки роста, повлиять на принятие решений, выявить проблемные зоны, планировать дальнейшие действия, ставить цели, развивать образовательное учреждение, актуализировать учебные программы, пересматривать их содержание, самостоятельно достичь соответствия критериям аккредитации или отчетности.