

Секция «Слабый и сильный искусственный интеллект в управленческих практиках»

Цифровой след

Научный руководитель – Назаренко Сергей Владимирович

Шаруханов Шарухан Гаджиевич

Студент (магистр)

Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного администрирования (факультет), Москва, Россия

E-mail: gogatun@gmail.com

Небывалое развитие сети Интернет и её проникновение в самые разные сферы жизни человека, несомненно, несёт множество положительных последствий. Цифровизация очень удобна - она позволяет совершать множество действий быстро и не выходя из дома, хотя ранее для совершения аналогичных действий от человека требовалось намного больше усилий и временных затрат (например, речь про совершение покупок онлайн).

Но нужно понимать, что у любого положительного явления есть и обратная сторона. И то же самое касается цифровизации.

Цифровизация в нашем случае - это возникновение, развитие и масштабное проникновение в жизнь человека технологий, связанных с использованием компьютерной техники и сети Интернет. Эти технологии могут значительно упрощать жизнь человека и даже повышать качество жизни, но их обратной стороной является тот самый цифровой след.

К цифровому следу могут относиться:

- история посещения интернет-ресурсов;
- отправляемая посредством электронных писем информация;
- сведения, заполняемые человеком о себе в онлайн-формах;
- материалы о человеке в социальных сетях;
- совершенные покупки в интернете.

То есть, под цифровой след может подпадать достаточно большой перечень данных либо о действиях человека в интернете, либо непосредственно о самом человеке. В последнем случае может иметься ввиду его платежная информация, адрес(-а) доставки, данные о предпочтениях и покупках, личные сведения, фотографии, публикации и пр.

Принято различать активный и пассивный цифровой след [1].

Примерами активного цифрового следа является намеренное размещение и распространение пользователем информации о себе. Как правило, имеются ввиду публикации пользователя от своего имени в социальных сетях, выкладывание материалов о себе. Но активный цифровой след может оставаться, например, при подписке на рассылку или же при условии согласия принимать файлы cookie в браузере.

Что касается пассивного цифрового следа, то от активного он отличается тем, что информация о пользователе собирается без его ведома - то есть, сам пользователь соответствующих инициатив не проявляет. Например, пассивный цифровой след имеет место, когда на веб-сайте собирается информация относительно того, сколько раз пользователи его посещали, откуда эти пользователи и каковы их IP-адреса. Процесс носит скрытый характер, и пользователи, скорее всего, даже не знают о нём. Ещё один пример - это анализ рекламодателями активностей человека в интернете и его предпочтений для показа того или иного рекламного контента, наиболее релевантного для данного человека.

Цифровой след достаточно постоянен. Он может иметь свою ценность для правоохранителей и государства, поскольку посредством цифрового следа будет проще отследить злоумышленника, воспользовавшись теми данными, которые он уже оставил о себе в интернете.

Впрочем, у данного примера существует ярко выраженная негативная сторона - цифровой след предоставляет государству и правоохранителям возможность следить за любым пользователем и нарушать неприкосновенность его частной жизни.

В разных странах мира существуют свои варианты и подходы к регулированию цифрового следа. В Китае, например, разработана система социального кредита [2]. Это своеобразная система оценки благонадёжности китайских и иностранных граждан, проживающих в КНР. Создана Всекитайская объединённая платформа кредитной информации, а деятельность по сбору информации о социальном кредите ведётся как центральным правительством, так и на уровне регионов. В целях удобства сбора информации каждому гражданину присвоен свой идентификационный код. Этот код необходим для совершения целого ряда действий - покупок онлайн, оформления проездных документов, сим-карт, получения ряда госуслуг.

В Китае выстроено регулирование цифровой личности (цифровой профиль, цифровой образ, цифровой след), которое существенно отличается от такового в Евросоюзе. Например, цифровой профиль человека характеризуется публичным характером в отличие от приватного характера, присущего цифровому профилю в развитых демократических государствах. Кроме того, в КНР на основе цифрового профиля формируются «красные» и «чёрные» списки лиц. «Красными» являются граждане, имеющие хороший социальный кредит и являющиеся примером для остальных. В «чёрном» же списке, напротив, находятся граждане, утратившие доверие.

Опыт китайского регулирования цифрового следа может быть оценен как неоднозначный и специфичный. С одной стороны, он позволяет государству и правоохранителям владеть максимально полной информацией о гражданине - весь цифровой след, по сути, фиксируется. С другой стороны, это создаёт опасную возможность злоупотреблений, вмешательства в частную жизнь человека. Сам же человек всегда осознаёт, что каждый его шаг в цифровом пространстве контролируется и вынужден жить с постоянной оглядкой на данный факт.

Отдельно интересен и опыт России в регулировании и отслеживании цифрового следа.

В нашей стране счёт законов и подзаконных актов, касающихся регулирования цифровой среды и интернет-коммуникаций, уже идёт на десятки. В качестве основного закона следует рассматривать №152-ФЗ «О персональных данных». Ценность данного закона, прежде всего, в том, что он определяет само понятие персональных данных [3].

Существуют некоторые важные поправки к федеральным законам, например, №264-ФЗ «О внесении изменений в ФЗ «Об информации, информационных технологиях и защите информации» [4]. Данный ФЗ примечателен тем, что урегулировал право на забвение в России. Согласно данному закону, оператор поисковой системы, по запросу клиента в определенных ситуациях, стал обязан прекратить выдачу ссылки на сайт с информацией о нём.

Кроме того, отдельного упоминания заслуживает биометрия.

21 декабря 2022 г. Госдумой принят проект федерального закона об информационной системе идентификации и аутентификации с использованием биометрических персональных данных физлиц [5].

В соответствии с данным документом запрещено хранить геномную информацию, а также определен закрытый перечень биометрических данных - это лицо и голос. Документ важен также и тем, что запрещает принуждение к сдаче биометрических данных, предусматривает гибкую систему отзыва ранее данного согласия на сдачу биометрии. Также не допускается трансграничная передача биометрических данных - они должны храниться только на территории РФ.

С 1 марта 2023 г. расширяется возможный спектр применения биометрии [6].

Так, биометрические данные будет возможно использовать при проведении промежуточной и итоговой аттестации в вузах, при проведении безналичных платежей (не более 1000 р.), аутентификации на портале госуслуг, а также заключении договоров об оказании услуг связи в интернете.

Биометрические данные - ещё одна составная часть электронного следа, поскольку хранятся они в цифровом виде. Следовательно, встаёт вопрос их защиты и безопасности.

Хотелось бы также отметить, что в современном цифровом пространстве перед пользователем остро стоит проблема цифрового следа, который, при неосторожном к нему отношении, может быть использован против него. Причём, проблемы могут возникнуть как в связи с действиями киберпреступников, так и в связи с претензиями от государства при совершении каких-либо предосудительных действий или распространения нежелательной информации. Подходы к регулированию цифрового следа могут существенно различаться в зависимости от страны пребывания. Поэтому внимательное отношение к цифровому следу - одно из главных условий интернет-грамотности и безопасности человека.

Источники и литература

- 1) Что такое цифровой след? // Kaspersky. URL: <https://www.kaspersky.ru/resource-center/definitions/what-is-a-digital-footprint>
- 2) Степанов О.А. Правовое регулирование генезиса цифровой личности / О.А. Степанов, М.М. Степанов // Правоприменение. – 2022. – Т. 6, № 3. – С. 19– 32. – DOI: 10.52468/2542-1514.2022.6(3).19-32.
- 3) Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (последняя редакция) // Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/
- 4) Федеральный закон "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и статьи 29 и 402 Гражданского процессуального кодекса Российской Федерации" от 13.07.2015 N 264-ФЗ (последняя редакция) // Консультант Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_182637/
- 5) Госдума приняла закон о единой биометрической системе, 21.12.2022 // ТАСС. URL: <https://tass.ru/ekonomika/16648113/amp>
- 6) Биометрия и авторизация на «Госуслугах» по-новому. Что меняется с 1 марта, 01.03.2023 // Banki.ru. URL: <https://www.banki.ru/news/lenta/?id=10980996>