

Секция «Проблемы конституционного строя и конституционного статуса личности»

**Алгоритм обработки данных и права человека: новые возможности или новые проблемы.**

**Научный руководитель – Маркова Елена Николаевна**

*Ростова Ульяна Дмитриевна*

*Студент (бакалавр)*

Московский государственный университет имени М.В.Ломоносова, Юридический факультет, Кафедра конституционного и муниципального права, Москва, Россия

*E-mail: ulia.rostova@mail.ru*

“software is eating the world”

Программы сегодня используются во многих сферах нашей жизни, в том числе бизнесом и социальными сетями. Наши действия в интернет-пространстве подчиняются четкому анализу цифрами и в целом определяют нашу жизнь в интернет-пространстве? Так что же тогда алгоритм? Наш помощник в бесконечном потоке информации или наоборот, ограничитель нашей свободы выбора. Ведь во многом алгоритмы опираются не только на сухие цифры, но и на взгляды, которые хочет донести компания до своих клиентов, поэтому здесь возникает вопрос, может ли алгоритм нарушить нормы конституционного права, кого привлекать к ответственности и как это не допустить

Потенциальными конституционными правами и свободами, которые может нарушить алгоритм, являются:

- право на неприкосновенность частной жизни, личную и семейную тайну
- Право на тайну переписки, телефонных переговоров и иных сообщений
- Сбор и хранение информации без согласия лица, а также ее анализ
- Свобода совести, свобода вероисповедания, право свободно выбирать, иметь и распространять религиозные и иные убеждения
- Свобода мысли и слова
- Свобода поиска, получения, передачи, производства и распространение информации
- Право на достоверную информацию об окружающей среде
- И другие

Важно также отметить, что алгоритмы часто анализируют поведения людей и берут их за основу своих действий. То есть, происходит некое навязывание общественного согласия или мнения большинства, с которым, когда столкнулся пользователь. Что может привести к некому «автоматизированному давлению» на человека, ему может подаваться только одна из сторона информации или же мнение только одной группы. Часто, выйти из этого просчета алгоритма достаточно сложно, что ведет к уже упомянутому навязыванию мнения или позиции, без сознательной на то воли человека. Когда мы смотрим телевизор, то мы можем переключить передачу, если она нам не нравится. В случае же с алгоритмом он всегда будет подстраиваться под наш возраст, пол, расу, место проживания. Таким образом, можно сделать вывод о том, что алгоритм навязывает нам некое согласие нашей социальной группы, показывает и призывает разделять ее усредненные интересы. Здесь можно отметить, например, алгоритмы рекомендаций платформы Tik Tok, которые как раз действуют на такой основе.

Таким образом, ключом к обеспечению соблюдения прав человека при использовании алгоритмов может быть понимание того, чего алгоритмы могут достичь, а чего не могут, и не позволять их использованию диктоваться только соображениями эффективности или результативности.

Важным являются вопросы, связанные с правом на неприкосновенность частной жизни. Алгоритмы позволяют анализировать огромный объем данных и используют системы отслеживания, чьи шаблоны записываются на «cookies». Все это создает проблемы конфиденциальности, и ограничивает человека. Посещенные сайты могут оказаться в так называемом открытом доступе, персональные данные могут быть украдены и направлены в преступное сообщество. Все это порождает некую свободу в несвободе, когда при выборе сайта мы всегда пытаемся спрогнозировать последствия его посещения, однако, в большинстве случаев это становится невозможным, так как осмыслить и предвидеть поведения алгоритмов, а также то, что скрывается за гиперссылкой бывает сложно.

В рекомендации Совета Европы по профилированию, отмечено, что имеется того, что профили, приписываемые субъекту данных, позволяют генерировать новые данные, в том числе путем агрегирования имеющихся. Затем эта информация может быть добыта с помощью алгоритмов, что создает риск крупномасштабного наблюдения как частными организациями, так и правительствами. Этой точки зрения придерживается и Совет ООН по правам человека, который 22 марта 2017 года с обеспокоенностью отметил, “что автоматическая обработка персональных данных для индивидуального профилирования может привести к дискриминации или решениям, которые в противном случае могут повлиять на осуществление прав человека, включая экономические, социальные и культурные права”

Наибольшую проблему во взаимодействии алгоритма, возникает при анализе взаимодействия и права на свободу выражения мнения. При очевидных преимуществах, которые дают алгоритмы, есть и недостатки, которые не стоит упускать. Так, в целом, ущемляется право на плюралистические дебаты. Так, контент, который алгоритмы посчитают «не интересным» или не подходящим для среднестатистического распространения, может быть автоматически отодвинут для всех пользователей. При этом, конечно, алгоритмы помогли услышать больше людей, создать общественное обсуждение и мировое сообщество единомышленников.

Главный вопрос, который возникает на данный момент - кого привлекать к ответственности за нарушение прав человека алгоритмами и как устранить нарушения, которые заложены в «сердце» алгоритма? За нарушение стоит привлекать создателя алгоритма - некоего IT специалиста, или же того, кто ввел в действие алгоритм на своей площадке? Или же нести ответственность нужно лишь тем, кто злоупотребляет данным, собранными алгоритмом? Все эти вопросы остаются нерешенными с точки зрения правового регулирования. Для прозрачности процедуры многие платформы публикуют типичные действия алгоритма, однако во многом сами несут ответственность за нарушения алгоритмов: Google, Facebook, Meta и другие. Здесь возникает проблема о надлежащей процедуре, которая соблюдается алгоритмами. Сложнее становится и при взаимоотношениях с иностранными платформами, многие из которых не имеют зарегистрированных ЮЛ на территории РФ.

Проблемы, которые связаны с автоматизированной обработкой данных, решаются с помощью законодательства о защите последних. На сегодняшний день используются такие подходы, как введение ограниченного “right to explanation” (право на объяснение) и другие права интернет-пользователей, которые являются новинкой для законодательства о защите данных. Однако существует значительная разница между конституционным правом на неприкосновенность частной жизни и регулированием защиты данных, все еще являющимся механизмом управления для охраны прав на неприкосновенность частной жизни и защиту персональных данных. В Российской Федерации многие из этих вопросов поставлены перед ФЗ «О персональных данных», однако, даже последние изменения этого закона не могут решить всех проблем, которые есть в современном обществе.

## Источники и литература

- 1) 1. "Конституция Российской Федерации" (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // СПС КонсультантПлюс
- 2) 2. Algorithms and Automated Decision-Making in the Content of Crime Prevention: A Briefing paper, 2016.
- 3) 3. Blokhin v. Russia, 13 April 2016, no 47152/06.
- 4) 4. German Federal Law on Data Protection, promulgated on 14 January 2003 (Federal Law Gazette I p. 66), and amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I p. 2814), available at: [https://www.gesetze-im-internet.de/bdsg\\_1990/\\_\\_\\_28b.html](https://www.gesetze-im-internet.de/bdsg_1990/___28b.html)
- 5) 5. Guidelines on the Protection of Individuals with regard to the Processing of Personal Data in a World of Big Data, 17 January 2017, available at: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806f06d0>
- 6) 6. Jespers v. Belgium, 15 October 1980, no 8404/78,
- 7) 7. Nguyen, Tien T., Pik-Mai Hui, F. Maxwell Harper, Loren Terveen, and Joseph A. Konstan. 2014. 'Exploring the Filter Bubble: The Effect of Using Recommender Systems on Content Diversity'. Pp. 677–686 in Proceedings of the 23rd International Conference on World Wide Web, WWW '14. New York, NY, USA: ACM
- 8) 8. Pasquale, Frank. 2015. The Black Box Society: The Secret Algorithms That Control Money and Information. Harvard University Press.
- 9) 9. Salduz v. Turkey, 17 November 2008, no 36391/02
- 10) 10. Tim O'Reilly, "The great question of the 21st century: Whose black box do you trust?", 13 September 2016, available at: [http://www.linkedin.com/pulse/great-question-21st-century-whose-black-box-do-you-trust-tim-o-reilly?trk=eml-b2\\_content\\_ecosystem\\_digest-hero-22-null&midToken=AQGexvwxq0Q3iQ&fromEmail=fromEmail&ut=2SrYDZ8lkCS7o1](http://www.linkedin.com/pulse/great-question-21st-century-whose-black-box-do-you-trust-tim-o-reilly?trk=eml-b2_content_ecosystem_digest-hero-22-null&midToken=AQGexvwxq0Q3iQ&fromEmail=fromEmail&ut=2SrYDZ8lkCS7o1)
- 11) 11. U.N. Human Rights Council Resolution on the Right to Privacy in the Digital Age, U.N. Doc. A/HRC/34/7, 23 Mar. 2017, para.2
- 12) 12. William Issac, Kristian Lum Kristian Lum and William Isaac (2016), To predict and serve? Significance, October 10, 2016, The Royal Statistical Society, available at: <http://onlinelibrary.wiley.com/doi/10.1111/j.1740-9713.2016.00960.x/epdf>
- 13) 13. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 02.07.2021) "О персональных данных" // СПС КонсультантПлюс