

використання об'єкта права інтелектуальної власності, з іншої — користувачі бажають отримати більше можливостей щодо вільного використання результатів творчої діяльності.

Специфіка конфліктів, які виникають в мережі Інтернет полягає у тому, що: такі конфлікти вимагають швидкого реагування; коло суб'єктів конфлікту може збільшуватись шохвилишно; «невидимість» суб'єктів конфлікту в мережі Інтернет.

Список використаних джерел

1. Базилевич В. Д. Інтелектуальна власність. – [Електронний ресурс]. – Режим доступу: <http://westudents.com.ua/glavy/19142-104-ntelcktualna-vlasnst-v-epohu-nternetu.html>
2. Беззуб І. Боротьба з інтернет-піратством в Україні: оцінки експертів. – [Електронний ресурс]. – Режим доступу: http://nbuvip.gov.ua/index.php?option=com_content&view=article&id=874:internet-piratstvo&catid=8&Itemid=350
3. Галіпін Л. Конфліктологія для управління. – Київ. – Шк. Світ., – 2008.
4. Іншин М. І. Трудові конфлікти та трудові спори у системі соціальних відносин. – Форум права – № 2– 200. – [Електронний ресурс]. – Режим доступу: www.nbuv.gov.ua

ЭПШАН Р. Е.

Национальный университет «Одесская юридическая академия»,
доцент кафедры права интеллектуальной собственности и корпоративного права,
кандидат юридических наук, доцент

ПРОБЛЕМА ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ СЕТИ ИНТЕРНЕТ

Сущность системной правовой проблемы идентификации пользователей в сети Интернет заключается в том, что в силу архитектурных особенностей сети Интернет взаимодействие между пользователями (реальными физическими лицами, действующими от своего лица или от лица иных представляемых ими лиц, в том числе юридических) объективно опосредовано, что приводит к сложностям в определении субъектов правоотношения в большинстве случаев.

Это может проявляться в самых разных практических ситуациях. Например, при взаимодействии пользователей социальной сети, при прочих равных условиях всегда отсутствует полная уверенность в том, что собеседник (а взаимодействие при этом может иметь и юридическое значение) действительно тот, за кого себя выдает посредством указания данных в своем профиле. В случае заключения договора в электронной

форме путем обмена электронными сообщениями, например, по электронной почте, если этому не предшествовали взаимодействия сторон, в результате которых были установлены достаточные процедуры верификации электронных сообщений, остается риск того, что сообщение направлено или получено не тем лицом. При совершении правонарушений в сети Интернет, как правило, крайне сложно установить лицо, которое размещало противоправную информацию, если только само оно не признает факт совершения действий или в деле не будет других доказательств.

Системность проблемы идентификации пользователей и ее общий характер подтверждается тем, что в той или иной форме она присутствует в любых правовых отношениях, опосредованных сетью Интернет и может быть выявлена в каждом случае взаимодействия. Данная проблема на практике разрешается на основании установленных законодательством, выработанных судебной практикой либо определенных на уровне саморегулирования (в том числе в форме договоров и обычаев) процедур верификации пользователей либо соответствующих юридических презумпций и фикций.

Опосредованность взаимодействия пользователей, лежащая в основе системной проблемы их идентификации, может рассматриваться на нескольких уровнях архитектуры сети Интернет. На *«физическом» уровне* такое взаимодействие опосредовано использованием компьютеров — в отсутствие каких-либо юридических презумпций и фикций наиболее точно взаимодействие в данном случае может быть описано исключительно как взаимодействие между двумя и более компьютерами.

Не всегда могут быть гарантии того, что на одном из этих компьютеров не действует автоматизированное программное обеспечение (бот). Однако, данная проблема может перейти в плоскость проблемы ответственности за автоматизированные действия: возможны ситуации, в которых действия бота будут рассматриваться осуществления действий или коммуникации со стороны пользователя. В таком случае можно говорить о наличии соответствующей юридической презумпции или фикции.

На *уровнях сети, Интернет-протокола и передачи данных* опосредованность взаимодействия определяется тем, что информация от одного пользователя поступает к другому пользователю различными способами и по различным сетевым маршрутам. Причем в ходе передачи как сама информация может быть перехвачена и изменена, так и сведения об источнике такой информации могут быть изменены, например, посредством использования *прокси-серверов* (сетевых служб, которые позволяют выполнять запросы к другим сетевым службам). Например, клиент (пользователь) может зайти на сайт как бы непосредственно, а может через прокси-сервер. В последнем случае при прочих равных условиях, со стороны «конечного» сервера именно

прокси-сервер будет выглядеть как источник запроса. Например, если какой-либо интернет-ресурс предлагает доступ только для пользователей, IP-адрес устройств которых определяется как относящийся к какой-либо определенной юрисдикции, то пользователь из другой юрисдикции может направить свой запрос через прокси-сервер «правильной» юрисдикции и таким образом попасть на сайт без ограничений.

На уровнях *приложений и контента* такая опосредованность взаимодействия, которая приводит к системной проблеме идентификации пользователей, выражается еще и в том, что взаимодействие в конечном счете осуществляется между различными программными приложениями за счет обмена содержащимся в них контентом, а не между пользователями как таковыми. На этом уровне проявляется проблема достоверности данных, указанных в тех же профилях социальных сетей.

Проблема идентификации пользователей по-разному разрешается на каждом уровне архитектуры сети Интернет. На каждом из уровней ее актуальность может быть разной, равно как и способы разрешения данной проблемы в каждой конкретной ситуации. Теоретическая значимость проблемы идентификации пользователей выражается в том, что она является основанием для уточнения и развития концепции субъекта правоотношения в сети Интернет. Классические подходы общей теории права и отраслевых юридических наук исходят из неявно выраженной презумпции непосредственного взаимодействия между субъектами. Вместе с тем в сети Интернет часто можно поставить вопрос о том, имеется ли в данном конкретном случае правоотношение в юридическом смысле в принципе, если субъекты правоотношения друг для друга часто являются неопределенными.

Практическая актуальность проблемы идентификации пользователей связана с тем, что в юридической практике необходимо либо **убедиться** в том, что правоотношения возникают с определенным субъектом (регулятивные правоотношения), либо **установить** такого субъекта (охранительные правоотношения). Например, в случае заключения договора с пользователем посредством сети Интернет в рамках какого-либо Интернет-сервиса часто возникает необходимость с достаточной степенью достоверности убедиться в том, что договор заключается с определенным лицом. Для этого могут использоваться различные инструменты верификации — подтверждение посредством электронного письма, направленного пользователем на адрес электронной почты, посредством смс-сообщения, направленного на указанный пользователем телефонный номер и т. д. Степень достоверности верификации каждого из таких способов, как правило, зависит от уже сложившихся юридически-значимых представлений о существующих презумпциях и фикциях, и редко является «абсолютно» (т. е. в том же смысле, как собственноручная подпись на бумажном носителе при предъявлении документа, удостоверяющего личность) достоверной.

Способы верификации пользователей сети Интернет в контексте проблемы их идентификации в значительной степени зависят от уровня развития технологий, и нередко появление новых, более достоверных способов «запускает» комплекс новых проблем, также требующих разрешения. Так, использование отпечатков пальцев на отдельных устройствах (например *iPhone*) развивает проблему идентификации пользователей до проблемы сбора, обработки и защиты биометрических персональных данных. В настоящее время проблема идентификации пользователей получает развитие на уровне правовых норм, регулирующих электронную подпись и персональные данные.

В данном контексте *электронная подпись* выступает в первую очередь как способ верификации пользователя сети Интернет и позволяет относительно (в зависимости от вида электронной подписи) достоверно его установить. Кроме того, отдельные используемые в электронных подписях технологии часто позволяют подтвердить и то, что в электронный документ не вносились изменения, после того как он был подписан электронной подписью.

Правовое регулирование *персональных данных* также следует рассматривать в контексте системной проблемы идентификации пользователей. При этом законодательство о персональных данных часто подходит к данной проблеме не со стороны субъекта правоотношения в сети Интернет, а со стороны определенного пользователя, который может выступать таким субъектом в сетевом взаимодействии. Ключевая составляющая законодательства о персональных данных — это само определение персональных данных, которое должно содержать научно обоснованные подходы к тому, какой набор данных позволяет идентифицировать субъекта и, соответственно, рассматриваться в качестве персональных.

На уровне саморегулирования в целом разрешение системной проблемы идентификации пользователей также развивается в направлениях совершенствования механизмов и подходов к верификации пользователей с использованием информационных технологий.