ІДЕНТИФІКАЦІЯ ОСОБИ, ЩО ЗДІЙСНИЛА ПОРУШЕННЯ АВТОРСЬКИХ ПРАВ НА ТВОРИ, ЩО РОЗМІЩЕНІ В МЕРЕЖІ ІНТЕРНЕТ ЗА ДОПОМОГОЮ P2P - МЕРЕЖ.

Зеров К.О.
Аспірант кафедри інтелектуальної власності юридичного факультету КНУ імені ~~тараса~~ Тараса Шевченка

Отформатировано: Шрифт: полужирный

Отформатировано: По центру, междустрочный, одинарный

Отформатировано: междустрочный, одинарный

Відносна анонімність користувачів мережі Інтернет має двоїсте значення. З одного боку, така діяльність певним чином сприяє порушенням авторського права та іншим правопорушенням. З іншого боку, питання анонімності інтернет-користувачів необхідно розглядати з урахуванням принципу пропорційності між правами інтелектуальної власності та правом на свободу вираження поглядів, правом на повагу до приватного і сімейного життя. Крім того, анонімність з'єднань зовсім не перешкоджає суспільно корисним діям (наприклад, правомірному розповсюдженню творів).

Процес ідентифікації особи, що вчинила порушення авторських прав на твори, що розміщені в мережі Інтернет, в зарубіжній науковій літературі прийнято поділяти на три стадії [1, с.36-37].

Перша стадія полягає у діяннях правоволодільця (його представника) щодо визначення і збирання IP-адрес та іншої інформації, що допоможе ідентифікувати особу порушника.

Для визначення і збирання IP-адреси порушника авторських прав у сфері функціонування P2P-мереж правоволодільці використовують такі методи:

* Непряме визначення користувачів, яке спирається на набір даних щодо пірів (англ. peers), що повертаються від торрент-трекеру.

* Пряме визначення полягає у підключенні за допомогою торрент-трекеру до користувачів, що розповсюджують певні файли та подальший обмін файлами з ними[2, с.8].

Обидва вказаних методи не виключають можливість помилки: було доведено, що будь-який користувач мережі Інтернет може отримати попередження за порушення авторських прав через штучну підміну IP-адреси, крім того такі попередження можуть отримати навіть комп'ютери та пристрої

(зокрема, мережеві принтери), за допомогою яких ніколи не відбувалось розповсюдження творів в мережі Інтернет[3, с.7].

Зауважимо, що існують певні технічні можливості, які дозволяють користувачам ускладнити (але не унеможливити) свою ідентифікацію. Наприклад, використання користувачами VPN чи PROXY серверів, використання "Даркнету" (англ. Darknet) / "цибулевої маршрутизації" (англ. Onion Routing, TOR) – послідовності проміжних мережевих вузлів з шифруванням інформації, що передається. [1, с.93]. Крім того, користувачі P2P- мереж використовують "чорні списки" з відомими IP-адресами правоволодільців (їх представників) для унеможливлення проведення такого моніторингу щодо них[3, с.4].

Друга стадія полягає у знаходженні відповідності IP-адреси визначеним абонентам (користувачам) окремих інтернет посередників.

У іноземній судовій практиці використовують різні підходи для вирішення означеного питання. Як свідчать матеріали судової практики США правоволодільці з метою захисту порушених авторських прав на твори, що розміщені в мережі Інтернет за допомогою торрент-трекерів, активно застосовують подання позовів проти невстановлених осіб (т.зв. "John Doe" в країнах англосаксонської правової сім'ї) – користувачів Bittorent трекерів із залученням інтернет-посередників для подальшої ідентифікації таких користувачів[4 с. 284].

У Великобританії з прийняттям Digital Economy Act у 2010 р. (DEA)[5], була встановлена процедура повідомлення правоволодільцем інтернет-посередника про онлайн порушення авторських прав (copyright infrigement report, CIR); процедура повідомлення інтернет-посередником свого користувача щодо отриманої скарги; та процедура з надання правоволодільцю переліку порушників (copyright infrigement list, CIL). При цьому вказаний перелік, згідно положень ст. 124-В закону DEA, не повинен містити відомостей, що прямо ідентифікують користувача. З 2006 по 2014 рр. в ЄС була чинною Директива 2006/24/ЄС "Про збереження даних, створених або оброблених при

наданні загальнодоступних послуг електронних повідомлень або громадських мереж зв'язку" [6]. Згідно положень ст.ст. 5 та 6 цієї Директиви інтернет-посередники зберігали, зокрема відомості щодо доступу в Інтернет, до електронної пошти та Інтернет-телефонії: дату і час підключення та відключення послуги доступу до мережі Інтернет разом з IP-адресою, присвоєною постачальником послуг доступу до Інтернету, а також ідентифікатор користувача абонента або зареєстрованого користувача; дату і час підключення та відключення послуги електронної пошти або через Інтернет, або Інтернет-телефонії. При цьому ці відомості повинні були зберігатися не менше шести місяців і не більше двох років. Така інформація надавалась на запит державних органів. Однак Європейський Суд Справедливості в об'єднаній справі C-293/12 та C-594/12 визнав зазначену Директиву нечинною з дати її прийняття, оскільки її положення суперечать принципу пропорційності по відношенню до інших основоположних прав людини і громадянина: праву на свободу вираження поглядів, праву на повагу до приватного і сімейного життя та праву захист персональних даних[7].

В Україні в 2010 р. були внесені зміни до Закону "Про телекомунікації"[8], зокрема до ч.2. ст.39: "Оператори, провайдери телекомунікацій зберігають та надають інформацію про з'єднання свого абонента у порядку, встановленому законом. Зауважимо, що спеціального встановленого законом порядку щодо витребування інформації щодо з'єднань абонента від інтернет-посередника в рамках цивільно-правового захисту станом на лютий 2016 року не передбачено. На нашу думку, в законодавстві необхідно передбачити процедуру щодо можливості досудового звернення правоволодільця (його представника) до інтернет-посередника з вимогою ідентифікації особи – абонента такого посередника, однак з урахуванням принципу пропорційності та встановленням відповідальності за зловживання отримання таких відомостей.

Третя стадія полягає у інформуванні чи направленні претензій особам щодо порушення ними авторських прав та можливості подання (чи

безпосередньо подання) проти них позовів. Як зазначає М. Філбі, ця стадія є найбільш складною, оскільки вимагає доведення двох складових, а саме: встановлення зв'язку між особою – абонентом, якому делеговано певну IP-адресу, та порушенням; доведення, що IP-адресу насправді було використано у несанкціонованому розповсюдженні творів[1, с.40].

На думку автора, по відношенню до ідентифікації особи – порушника авторських прав виключно за допомогою IP-адреси слід ставитись з певними застереженнями, оскільки IP-адреса надає інформацію тільки щодо джерела з'єднання - певного місця (а не особи), з якої невизначена кількість апаратних засобів може встановити з'єднання до мережі Інтернет. Наприклад, поштовою скринькою чи телефонним номером також може скористуватись невизначена кількість користувачів. На зазначену проблему звертає увагу і зарубіжна судова практика. [9, п.103].

У зв'язку з цим необхідно зазначити, що IP-адреса не є єдиним можливим ідентифікатором користувачів мережі Інтернет. Зокрема, крім IP-адреси існує ще MAC-адреса. Якщо IP-адреса може надати відомості щодо місця знаходження, то MAC є унікальною апаратною адресою для кожного пристрою, з якого відбувається підключення до мережі Інтернет. При цьому одній IP-адресі може відповідати одночасно лише одна MAC-адреса пристрою, що підключений до мережі Інтернет, наприклад, маршрутизатора користувача (зазначені технічні відомості наявні у інтернет-посередників).

Враховуючи вищенаведене, вважаємо, що саме для ідентифікації особи – порушника (а не місця, в якому вчинене порушення) авторських прав на твори, що розміщені в мережі Інтернет, виключно за допомогою використання IP-адреси недостатньо і необхідно використовувати додаткові докази) для встановлення причинно-наслідкового зв'язку між особою – абонентом, якому делеговано певну IP-адресу, та порушенням авторських прав.

ЛІТЕРАТУРА

Отформатировано: украинский

1. Filby M. Regulating File Sharing: Using Law, Internet Architecture, Markets and Norms to Manage the Non-Commercial Sharing of Digital Information / M. Filby. – Lexington, KY, USA, 2015. – 248 с.
2. Harding T. BitTorrent tracking as a means of detecting illegal file-sharing / Tom Harding. // E-Commerce Law & Policy. – 2013, February. – С. 8–9.
3. Piatek M. Challenges and Directions for Monitoring P2P File Sharing Networks or Why My Printer Received a DMCA Takedown Notice [Електронний ресурс] / M. Piatek, T. Kohno, A. Krishnamurthy – Режим доступу до ресурсу: http://dmca.cs.washington.edu/dmca_hotsec08.pdf.
4. Karunaratne S. The Case Against Combating BitTorrent Piracy Through Mass John Doe Copyright Infringement Lawsuits / Sean B. Karunaratne. // Michigan Law Review. – 2012. – №111. – С. 283–309.
5. Digital Economy Act 2010 [Електронний ресурс] – Режим доступу до ресурсу: http://www.legislation.gov.uk/ukpga/2010/24/pdfs/ukpga_20100024_en.pdf.
6. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications net. // Official Journal of the European Union. – 2006. – №105. – С. 54–63.
7. The Court of Justice declares the Data Retention Directive to be invalid [Електронний ресурс] – Режим доступу до ресурсу: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf.
8. «Про телекомунікації», закон України від 18.11.2003 № 1280-IV // Відомості Верховної Ради України (ВВР), 2004, N 12, ст.155. (зі змінами).
9. Decision of England and Wales High Court (Chancery Division) in case Golden Eye (International) Ltd & Anor v Telefonica UK Ltd., Case No: HC11C03290, 26 March 2012 [Електронний ресурс] – Режим доступу до ресурсу: http://www.bailii.org/ew/cases/EWHC/Ch/2012/723.html.

Отформатировано: русский
Отформатировано: русский
Отформатировано: русский
Отформатировано: русский
Отформатировано: русский
Отформатировано: русский
Отформатировано: русский
Отформатировано: русский
Отформатировано: русский
Отформатировано: русский
Отформатировано: русский
Отформатировано: русский