Антон Серго
«Интернет и право»

(http://internet-law.ru/book)

«Бестселлер», 2003 - 272 с. ISBN 5-98158-002-X

ГЛАВА 9. ПЕРСОНАЛЬНАЯ ИНФОРМАЦИЯ В СЕТИ

Эта мысль — украденный цветок,
просто рифма ей не повредит:
человек совсем не одинок,
кто-нибудь всегда за ним следит.
И. Губерман

Сегодня всемирная сеть Интернет вобрала в себя все позитивное и негативное информационное наполнение — это всемирная библиотека и склад компромата, глобальный информационный справочник и террористическое пособие. В Сети каждый без труда найдет то, что ему нужно, в том числе о том, о ком нужно.

Глава посвящена отдельным аспектам сетевой информации, делающей пользователя наиболее уязвимым со стороны недоброжелателей.

Государственный контроль

Как известно, у нас в стране активно используется «Система оперативно-розыскных мероприятий» (сокращенно — СОРМ и СОРМ-2) — специализированный программно-технический комплекс, устанавливаемый у провайдеров и перехватывающий во всем потоке трафика сообщения и материалы, могущие представлять интерес для органов, осуществляющих оперативно-розыскную деятельность.

Действующее законодательство об оперативно-розыскной деятельности предусматривает в числе оперативно-розыскных мероприятий — контроль почтовых отправлений, телеграфных и иных сообщений, прослушивание телефонных переговоров, снятие информации с технических каналов связи. В соответствии со ст. 6 федерального Закона «Об оперативно-розыскной деятельности», при осуществлении оперативно-розыскных мероприятий, связанных с контролем почтовых отправлений, телеграфных и иных сообщений, прослушиванием телефонных переговоров с подключением к станционной аппаратуре предприятий, учреждений и организаций независимо от форм собственности, физических и юридических лиц, предоставляющих услуги и средства связи, со снятием информации с технических каналов связи, они проводятся с использованием оперативно-технических сил и средств органов федеральной службы безопасности, органов внутренних дел и, в пределах своих полномочий, федеральных органов налоговой полиции в порядке, определяемом межведомственными нормативными актами или соглашениями между органами, осуществляющими оперативно-розыскную деятельность. Для осуществления таких мероприятий могут использоваться технические средства.

В соответствии со ст. 8 указанного Закона, проведение оперативно-розыскных мероприятий, которые ограничивают конституционные права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а также право на неприкосновенность жилища, допускается на основании судебного решения и при наличии информации:

1) о признаках подготавливаемого, совершаемого или совершенного противоправного деяния, по которому производство предварительного следствия обязательно;

2) о лицах, подготавливающих, совершающих или совершивших противоправное деяние, по которому производство предварительного следствия обязательно;

3) о событиях или действиях, создающих угрозу государственной, военной экономической или экологической безопасности Российской Федерации.

Кроме того, в случаях, не терпящих отлагательства и могущих привести к совершению тяжкого преступления, а также при наличии данных о событиях и действиях, создающих угрозу государственной, военной, экономической или экологической безопасности Российской Федерации, на основании мотивированного постановления одного из руководителей органа, осуществляющего оперативно-розыскную деятельность, допускается проведение данных оперативно-розыскных мероприятий с обязательным уведомлением суда (судьи) в течение 24 часов. В течение 48 часов с начала проведения оперативно-розыскного мероприятия орган, его осуществляющий, обязан получить судебное решение о проведении такого оперативно-розыскного мероприятия либо прекратить его проведение.

Такова правовая база использования СОРМ, правовая база установки основывается на федеральном Законе «Об органах федеральной службы безопасности в Российской Федерации». Он предусматривает, что физические и юридические лица в Российской Федерации, предоставляющие услуги почтовой связи, электросвязи всех видов, в том числе систем телекодовой, конфиденциальной, спутниковой связи, обязаны по требованию органов федеральной службы безопасности включать в состав аппаратных средств дополнительные оборудование и программные средства, а также создавать другие условия, необходимые для проведения оперативно-технических мероприятий органами федеральной службы безопасности.

Законодательство об оперативно-розыскной деятельности предусматривает, что оперативно-розыскные мероприятия, связанные с ограничением права личности на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а также права на неприкосновенность жилища, осуществляются по конкретному решению в отношении конкретного лица в течение определенного в решении срока. Причем решение о проведении таких мероприятий принимает суд. Однако установленный порядок осуществления СОРМ идет вразрез с этими положениями и дает органам, осуществляющим оперативно-розыскную деятельность, возможность постоянно контролировать информацию, передающуюся по телекоммуникационным сетям.

Подобные системы функционируют и в других странах. Например, американский «Эшелон» координирует действия нескольких спецслужб: британской Government Communications Headquarters (GCHQ), канадской Communications Security Establishment (CSE), австралийской Defense Signals Directorate (DSD) и новозеландской Government Communications Security Bureau (GCSB). Причем полу-

ченная информация используется не только для ловли преступников, но и для промышленного шпионажа. По имеющейся информации, именно так был расстроен в 1994 году дорогой контракт на закупку Саудовской Аравией французских самолетов, доставшийся американскому конкуренту. Французы уверены, что узнать засекреченные условия сделки американцы смогли с помощью «Эшелона». Подобный случай не единственный.

В конце прошлого века, помимо глобальной системы «Эшелон» в США была запущена в эксплуатацию внутригосударственная система слежения за пользователями Сети — Carnivore (DCS-1000). Официальное признание подобной системы вызвало бурю эмоций в демократическом государстве. Общественные организации выступили с требованием опубликовать исходный код программы и другие технические детали, а также юридическое обоснование использования такой системы. Более мягким было требование предоставить экспертам доступ к коду программы, чтобы выяснить, действительно ли программа отслеживает действия лишь подозреваемого или всех пользователей. Однако ФБР отказалось открыть код программы, мотивируя это возможностью взлома программы, а также нарушением авторских прав создателей.

Как видно, существование подобных систем вызывает справедливые нарекания и возмущение общественности, но, несмотря на явно незаконный характер такой деятельности, она осуществляется как в тоталитарных, так и в ведущих демократических государствах.

Компромат в Сети

Последнее время, накануне крупных политических событий, Сеть используется для «сброса компромата». Легкость и оперативность размещения информации, ничтожная стоимость этой операции делают эту деятельность наиболее простой и массовой. Какова юридическая оценка сетевого компромата?

Прежде всего, к любому сайту применимы отдельные нормы законодательства о СМИ, что было показано в соответствующем разделе. Кроме того, подобные материалы подпадают по действие статей Уголовного кодекса, например ст. 129 «Клевета» (распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию), ст. 130 «Оскорбление» (унижение чести и достоинства другого лица, выраженное в неприличной форме), ст. 137 «Нарушение неприкосновенности частной жизни» (незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, если эти деяния совершены из корыстной или иной личной заинтересованности и причинили вред правам и законным интересам граждан), ст. 138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан».

«Жетоны» (Cookie)

Помимо уже описанного слежения и сбора информации о пользователях Интернета, осуществляемого государственными структурами, подобное проводят различные сетевые ресурсы. Наибольший интерес в этой сфере проявляется к технологии, использующей «жетоны» (cookie)[1]. По содержанию, cookie это файл с небольшим блоком текстовой информации о компьютере пользователя, которая (после обработки программным обеспечением сайта) возвращается на компьютер пользователя и хранится там от нескольких минут до нескольких лет[2].

Теоретически, cookie выполняют положительную функцию — автоматизируют процесс работы пользователя с интернет-сайтом, передавая ему одну и ту же информацию (имя пользователя, пароль, настройки) без необходимости каждый раз запрашивать ее у пользователя. Однако cookie-файлы могут содержать практически любую информацию о пользователе и использоваться различными интернет-ресурсами, передавая друг другу некоторую информацию о пользователе.

Отдельного упоминания заслуживают так называемые системы статистики, размещающие свой код на страницах сайтов. При обращении пользователя к сайту, где расположен счетчик, система анализирует информацию об обратившемся компьютере (пользователе)[3], идентифицируя его по уникальному номеру.

Учитывая широкий охват Интернета, подобные системы позволяют совершенно четко отслеживать (и анализировать) веб-серфинг каждого пользователя (по каким сайтам ходит, когда и в какое время, что пропускает, на чем останавливается подолгу). Исходя из этого можно сделать массу выводов: о круге интересов, хобби, деятельности, примерном уровне доходов, вкусах и предпочтениях.

Не только наличие, но и использование подобной информации не отрицается владельцами «счетчиков». В описании возможностей системы Spylog указывается: «Допустим, вы продаете апельсины. Вводите слово «апельсин» и получаете выборку всех пользователей, которые когда-либо вводили это слово в поисковик. Далее мы смотрим, где чаще всего бывают эти люди. В результате клиент может выбрать десяток сайтов, где реклама будет наиболее результативна, где чаще всего бывают люди, которых интересуют апельсины. Такие уникальные сервисы позволяют предоставлять наши базы данных».

---

[1] Достижение указанных целей возможно и на основе других технологий.

[2] Пользователь без труда может обнаружить эти файлы в одноименной директории своего компьютера.

[3] Объем запрашиваемой информации неизвестен, но на сайте одного из популярных «счетчиков» — Spylog указано, что предоставляется более 600 видов статистики, из чего можно сделать вывод об объеме запрашиваемой и анализируемой информации. Причем на пике своей популярности этот «счетчик», по словам владельцев, охватывал 95% российского Интернета, а сейчас его услугами пользуется более 250 тысяч сайтов.

При этом указывается, что система «не идентифицирует людей — в этом и есть защита личной информации». Однако собранная информации о браузере и его владельце более чем достаточная для идентификации личности. Все это без труда могут использовать как государственные, так и негосударственные структуры (для сбора различной информации, в том числе компрометирующей).

В принципе, у пользователя есть возможность отключить прием «cookie»-файлов на свой компьютер, но для нормальной работы со многими сетевыми ресурсами их использование (прием) является необходимым. Кроме того, по умолчанию, на компьютере прием cookie-файлов всегда разрешен. Для их отключения требуются определенные знания и навыки. Поэтому представляется, что включение функции приема cookie-файлов юридически нельзя рассматривать как согласие пользователя на сбор, обработку и дальнейшее распространение информации о нем (в том числе персональных данных). В то же время весьма целесообразным было бы рекомендовать (по аналогии с зарубежными системами) включать небольшой информационный текст в распространяемый код счетчика, который если и не выводился на экран, то хотя бы имел четкую ссылку на такую информацию.

Правовой аспект публикации персональных данных в Сети

Прежде чем давать строго правовую оценку сбору, обработке и распространению персональных данных в Интернете, следует обратить внимание, что техническая основа Сети такова, что почти любое пребывание в ней является прозрачным и открытым для других лиц. Когда автор получил «загадочное» послание, его отправитель был вычислен быстро и точно, несмотря на пользование услугами интернет-кафе. Все это заняло считанные минуты и не потребовало привлечения специалистов или особых программно-технических средств (и уж тем более правоохранительных органов).

Возвращаясь к вопросу правового режима информации о гражданине (персональных данных), то следует, прежде всего, указать, что их защита закреплена на конституционном уровне. Как указывается: «Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения»[4], а также «сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются»[5].

[4] См. ст. 23 Конституции РФ.

[5] См. ст. 24 Конституции РФ.

Более подробно правовой статус персональных данных[6] определяется федеральным законом от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации». В нем же содержится положение, аналогичное конституционному: «Не допускаются сбор, хранение, использование и распространение информации о частной жизни, а равно информации, нарушающей личную тайну, семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме как на основании судебного решения».

К сожалению, закон носит в большей степени декларативный характер. Его принятие было важным шагом на пути формирования правовой базы персональных данных. Но реалии сегодняшнего дня требуют корректировки его и принятия иных нормативно-правовых актов в этой сфере, а также завершения процесса присоединения России к Конвенции о защите личности в связи с автоматической обработкой персональных данных (Страсбург, 28 января 1981 г.).

Ответственность за незаконный сбор и/или использование персональных данных установлена Кодексом РФ об административных правонарушениях (ст. 13.11) и Уголовным кодексом РФ (ст ст. 137, 138).

В отличие от нашей страны, в европейских странах этот вопрос стоит достаточно остро и по нему принимаются соответствующие нормативно-правовые акты. Представляется, что это отставание наши законодатели будут наверстывать в самое ближайшее время.

В западной терминологии под неприкосновенностью частной жизни понимается достаточно широкое понятие, включающее возможность контролировать то, что о субъекте знают другие, когда они об этом узнают и что они могут делать с этой информацией.

Как уже было показано ранее, современные компьютерные технологии без особого труда позволяют пристально следить и быть в курсе каждого шага любого пользователя Сети, собирая о нем массу информации.

Для того, чтобы обеспечить неприкосновенность частной жизни любого лица, в том числе и пользователя Сети, Европейским союзом была принята Директива № 95/46/ЕС «О защите данных». В соответствии с ней, любая организация должна предоставить следующие возможности пользователю, в отношении предоставленной им информации[7]:

---

[6] Персональные данные (информация о гражданах) — сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность. Персональные данные относятся к категории конфиденциальной информации. Ст. 2, ст. 11 ФЗ от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации».

[7] Подробнее см. Скиба В. Итоги Второй международной конференции по электронной коммерции и интеллектуальной собственности // http://www.russianlaw.net/law/doc/a134.htm

1) **уведомление** (организация должна уведомлять лицо о целях сбора и использования информации о нем, предоставить контактную информацию, перечислить третьих лиц, которым эта информация передается, и информацию о средствах и возможностях ограничить эту передачу);

2) **выбор** (организация должна предоставить лицу возможность выбрать, будет ли их личная информация предоставляться третьим лицам и использоваться для других целей, чем те, для которых она собиралась);

3) **передача** (организация должна применять правила уведомления и выбора для передачи и осуществлять передачу только в том случае, если другая организация принимает принципы Директивы Евросоюза или иные аналогичные принципы);

4) **доступ** (лицо должно иметь доступ к своей персональной информации и возможность исправлять, добавлять или удалять эту информацию);

5) **безопасность** (организация должна принимать меры для защиты информации от потери, неправомерного использования или неправомерного доступа к ней);

6) **достоверность** информации (информация должна отвечать целям, для которых она используется, и организация должна применять разумные действия, чтобы обеспечить относимость, правильность и полноту информации);

7) **обеспечение выполнения принципов** (должна существовать процедура для независимого и доступного защитного механизма, включающего ответственность за возможные нарушения).

Несмотря на все сказанное, абсолютное соблюдение всех этих положений сегодня не представляется возможным. Как уже говорилось, техническая основа Сети такова, что почти любое пребывание в ней является прозрачным и открытым для других лиц. Пользователь, подключаясь к Сети, прекрасно осознает это и готов идти на этот риск. Абсолютное соблюдение законодательства о персональных данных потребовало бы программной и технической перестройки Сети, что, как следствие, лишило бы ее пользователей массы удобств и сервисов, но соблюдение основных принципов (рассмотренных выше) представляется не только возможным, но и необходимым.