Эфемерная улика. Электронные доказательства в странах общего права

Как в повседневной жизни, так и в коммерческой практике сегодня огромную роль играют электронные средства коммуникации и хранения информации. Никто больше не ведет бухгалтерского учета в гроссбухах, все данные сразу заносятся в компьютер. Почти никто не пишет коммерческому контрагенту писем на бумаге, вся переписка идет по электронной почте. И так далее.

Конечно, право не может оставаться глухим к этим веяниям времени. В том числе это относится и к доказательственному праву, регулирующему допустимость доказательств в судебном процессе.

Когда-то электронные данные могли казаться слишком эфемерными, чтобы всерьез рассматривать их как доказательства для суда. Как можно представить суду какой-то набор из нулей и единиц! Но сегодня все изменилось. Поскольку электронные записи и электронная переписка играют столь серьезную роль в реальной жизни, то они неизбежно становятся и предметом судебного анализа и оценки.

Соответственно, суды всех (вероятно) стран мира в настоящее время в принципе признают электронные данные допустимыми доказательствами для целей как гражданского, так и уголовного процесса. В этой статье мы обсудим позицию судов общего права по этому вопросу.

***

Начну с обширной цитаты из решения[1] суда Пенсильвании от 2005 года, которая во многом объясняет отношение судов общего права к электронным доказательствам.[2]

«По существу, заявитель хотел бы, чтобы мы создали целый раздел права, просто чтобы покрыть сообщения электронной почты и мгновенные сообщения. Аргумент состоит в том, что такие сообщения электронной почты и мгновенные сообщения по сути своей недостоверны (inherently unreliable) ввиду своей относительной анонимности, а также того факта, что хотя электронное сообщение может быть прослежено до конкретного компьютера, оно редко может быть связано с конкретным автором с какой-либо определенностью. Если только предполагаемый автор не отправлял сообщение на глазах свидетеля, всегда есть возможность того, что оно не от того человека, который указан как автор. Как заявитель правильно отмечает, любой, кто имеет правильный пароль, может получить доступ к электронной почте другого лица и посылать сообщения якобы от этого лица. Однако те же неопределенности существуют с традиционными письменными документами. Подпись может быть подделана; письмо может быть напечатано на пишущей машинке другого лица; фирменный бланк может быть украден или подделан. Мы полагаем, что сообщения электронной почты и подобные виды электронных сообщений могут быть надлежащим образом аутентифицированы в существующих правовых рамках ... . Мы не видим нужды в придумывании уникальных правил для допустимости (unique rules of admissibility) электронных доказательств, таких как мгновенные сообщения; они могут быть оценены на индивидуальной (case-by-case) основе, как любой другой документ, для определения того, продемонстрировано ли достаточное основание (adequate foundational showing) для признания их относимости и подлинности.»

***

[1] In Re F.P., 878 A.2d 91, 95-96 (Pa. Super. Ct. 2005).
[2] См.: *Miskel E.* Admissibility of Digital Evidence in a Family Case. 2015. <http://www.emilymiskel.com/pdfs/2015FamilyJustice.pdf>.

Сегодня суды многих стран мира рутинным образом принимают в качестве доказательств сообщения электронной почты, СМС-сообщения, переписку в чате, содержание веб-сайтов, электронные записи систем наблюдения, файлы из компьютера обвиняемого по уголовному делу и т.п.

Такие электронные данные могут быть представлены в суде заинтересованной стороной, которая ими обладает (например, имеет их на своем компьютере). Или заинтересованная сторона может истребовать эти данные от оппонента (если они хранятся на его компьютере). Или заинтересованная сторона может истребовать эти данные от лица, не являющего стороной по делу (например, от провайдера, предоставляющего услуги электронной почты).

Разумеется, истребование электронных данных от других лиц, так же как и истребование бумажных документов или любых иных доказательств, осуществляется лишь в случаях, предусмотренных процессуальным законодательством соответствующей юрисдикции. Законодательство многих юрисдикций общего права, особенно в США, предоставляет для такого истребования доказательств в гражданском процессе весьма широкие возможности (в отличие от многих континентально-европейских юрисдикций, где подобные возможности куда более ограничены).

По большому счету, вопрос при этом лишь в том, каким образом такие электронные данные, обычно недоступные непосредственному чувственному восприятию, могут быть представлены суду. Может ли судья приобщить к делу электронный файл? Ну и, конечно, в том, насколько суду стоит этим данным доверять: ведь электронную запись зачастую очень легко изменить!

***

Как правило, к делу приобщаются не сами файлы, а их «распечатки» (там, где это возможно). Ведь распечатку на бумаге куда легче приобщить к делу! Но если речь идет, например, о записи системы видеонаблюдения, то ее придется воспроизвести и продемонстрировать суду или присяжным, которые будут оценивать данное доказательство.

Возможно, в случае гражданско-правовых споров (далее мы говорим только о них) наиболее актуальным на практике является вопрос предоставления суду сообщений электронной почты, являющихся частью переписки между сторонами. Технически нет проблемы в том, чтобы распечатать такие сообщения (и, если нужно, вложенные в них файлы) с компьютера одной из сторон. Проблема лишь в том, как эту распечатку заверить для суда.

В России для этого обычно пользуются услугами нотариуса, что не всегда удобно и эффективно. В странах же общего права эта проблема обычно решается так же, как и проблема аутентификации любых других доказательств.

По общему правилу подлинность доказательства подтверждается в процессе свидетелем, имеющим знание из первых рук об этом доказательстве. Например, истец, ссылающийся на полученное от ответчика электронное сообщение, под присягой подтверждает в процессе подлинность представленной им суду копии.

Но на практике, поскольку доказательства сегодня обычно раскрываются на предварительных стадиях гражданского процесса, то истец заранее представит копию этого сообщения, заверенную аффидевитом самого истца (то есть письменным подтверждением подлинности документа, данным под присягой). Если же данные получены от третьего лица, то именно это лицо подтверждает подлинность своим аффидевитом.

Если оппонент не оспаривает подлинности сообщения, этого будет вполне достаточно. Если же оппонент оспаривает подлинность, он может подвергнуть автора аффидевита перекрестному допросу в процессе. Оппонент также может представить свои доказательства, например, свою распечатку того же письма, заверенную своим аффидевитом.

Казалось бы, сфабриковать электронное сообщение ничего не стоит. Но поскольку в основных странах общего права существует весьма суровая уголовная ответственность за дачу ложных показаний под присягой, а также весьма суровая профессиональная ответственность адвокатов за содействие в фабрикации доказательств, то предоставление суду заведомо ложных доказательств этих странах – большая редкость. Во всяком случае, в серьезных коммерческих спорах.

Помимо прочего, следует иметь в виду, что в случае, когда стороной является коммерческая фирма, ее сотрудник, распечатывающий файл из своего компьютера, вряд ли для блага родной фирмы захочет сесть в тюрьму за подписание ложного аффидевита!

***

Допустимость электронных доказательств, разумеется, не означает, что судья или присяжные непременно обязаны принимать их содержание за чистую монету. Как и в случае бумажных документов, содержание электронных файлов оценивается наряду с другими доказательствами, взятыми в совокупности, с необходимыми оговорками насчет того, насколько заслуживает доверия тот или иной свидетель. В частности, может потребоваться доказать, что (например) именно ответчик, а не кто-то другой, имевший доступ к его компьютеру, написал спорное сообщение!

В этом смысле электронные доказательства не вносят ничего нового в доказательственное право.

По большому счету, несколько модифицируются лишь правила аутентификации (подтверждения подлинности) доказательств, а также положение общего права, известное как «правило наилучшего доказательства».

Это традиционное правило (best evidence rule) гласит, что если существует оригинал документа, то суду должен быть представлен именно оригинал, а не копия (идея, очевидно, в том, что оригинал труднее подделать). Следует заметить, что во многих юрисдикциях « правило наилучшего доказательства» сегодня применяется с большими оговорками или вовсе не действует.

Что касается электронных доказательств, если сторона полагалась на распечатку электронных данных, то именно эта распечатка (а не оригинальный электронный файл) признается «наилучшим доказательством».

***

Доказательственное право различных стран общего права не идентично, но во многих аспектах сходно. Подход стран общего права к вопросу допустимости электронных доказательств можно продемонстрировать при помощи документа, который называется «Модельный закон об электронных доказательствах» (Model Law on Electronic Evidence).

Этот модельный закон был разработан в 2002 году по инициативе министров права и генеральных прокуроров малых стран Содружества наций. Закон написан в основном по образцу канадского Единообразного закона об электронных доказательствах (Canada Uniform Electronic Evidence Act), с использованием положений сингапурского доказательственного права, а также некоторых разработок ЮНСИТРАЛ (UNCITRAL).

Закон состоит всего лишь из 12 статей (далее, если иное не оговорено, ссылки делаются на статьи этого закона). Ниже перечисляются некоторые наиболее важные его положения (в несколько сокращенном варианте).

Прежде всего, как водится, в законе определяются термины. Ключевое понятие «электронная запись» определяется как данные, записанные на любом носителе в компьютерной системе, которые могут быть считаны или восприняты лицом или компьютерной системой (ст. 2).

Согласно закону, никакие правила доказательственного права не должны использоваться для признания недопустимыми доказательствами электронные записи лишь в силу того, что это – электронные записи (ст. 3).

В законе явно говорится, что он не изменяет никаких правил доказывания, за исключением правил аутентификации и правила «наилучшего доказательства» (ст. 4).

Лицо, желающее представить электронную запись в качестве доказательства, несет бремя доказывания его подлинности надлежащими доказательствами (ст. 5).

Применительно к системам электронной записи (система видеонаблюдения и т.п.), если применимо «правило наилучшего доказательства», то его можно выполнить, доказав достоверность (integrity) такой системы (ст. 6(1)).

Если сторона в своих действиях полагалась на распечатку электронных данных, то эта распечатка приравнивается к оригиналу для целей «правила наилучшего доказательства» (ст. 6(2)).

Если нет доказательств иного, то достоверность (integrity) системы электронной записи презюмируется, если:

- соответствующая компьютерная система функционировала надлежащим образом (properly);
- запись сделана системой, контролировавшейся процессуальным оппонентом стороны, представляющей доказательство; или
- запись сделана в ходе обычной деятельности лицом, не являющимся стороной процесса (ст. 7).

Обстоятельства, относящиеся к достоверности и корректности работы систем электронной записи, могут быть установлены при помощи аффидевитов с формулировкой «насколько мне известно» (the best of the deponent’s knowledge or belief) (ст. 9).

Автор такого аффидевита может быть подвергнут перекрестному допросу заинтересованной стороной (ст. 10).

Стороны могут заключить соглашение о допустимости тех или иных электронных доказательств (ст. 11).

Если положение доказательственного права требует «подписи» на документе, то в случае электронной записи этому требованию удовлетворяет «электронная подпись» (electronic signature), которая может быть подтверждена «любым образом» (may be proved in any manner). В том числе демонстрацией того, что для выполнения транзакции лицу надо было пройти определенную процедуру или ввести определенные символы (ст. 12).

Здесь под «электронной подписью», по-видимому, понимается нечто вроде пароля. Однако следует иметь в виду, что во многих юрисдикциях «электронной подписью» может быть названо и просто имя автора электронного сообщения, набранное им в конце сообщения. То есть у них «электронная подпись» - это совсем не то, что у нас.

***

Как видим, в странах общего права вопросы, связанные с допустимостью электронных доказательств, неплохо продуманы и в целом урегулированы. Сторона без проблем может представить электронные доказательства в суд. Заверяет она их, как правило, своим собственным аффидевитом. Если доказательства хранятся в компьютере оппонента или третьей стороны, они могут быть истребованы в общем порядке, предусмотренном для истребования доказательств. Подлинность электронных доказательств обеспечивается весьма серьезной ответственностью за ложь в суде. Содержание и авторство представленного документа оценивается судом на основании всех доказательств в совокупности.