РЕКОМЕНДАЦИЯ N R (99) 5 КОМИТЕТА МИНИСТРОВ ГОСУДАРСТВАМ-ЧЛЕНАМ СОВЕТА ЕВРОПЫ ПО ЗАЩИТЕ НЕПРИКОСНОВЕННОСТИ ЧАСТНОЙ ЖИЗНИ В ИНТЕРНЕТЕ

Утверждено Комитетом Министров 23 февраля 1999 года

Преамбула

Комитет Министров на основании полномочий, определенных Статьей 15.b Устава Совета Европы (994_001), учитывая, что цель Совета Европы заключается в достижении большего единства между его членами;

принимая во внимание развитие новых технологий, новых средств передачи информации и интерактивных услуг;

понимая, что такое развитие повлияет на деятельность общества в целом и на отношения между людьми, в частности предоставляя расширенные возможности передачи и обмена информацией на национальном и международном уровнях;

осознавая преимущества, которые получат пользователи новых технологий при таком развитии;

учитывая, однако, что технологическое развитие и широкое распространение сбора и обработки персональных данных на информационных магистралях влечет опасность нарушения неприкосновенности частной жизни личности;

принимая во внимание, что технологическое развитие также делает возможным внести вклад в соблюдение основных прав и свобод и, в особенности, права личности на неприкосновенность частной жизни при обработке персональных данных;

сознавая необходимость развития методов, обеспечивающих анонимность субъектов данных и конфиденциальность информации, циркулирующей на информационных магистралях, при соблюдении прав и свобод других личностей и ценностей демократического общества;

сознавая, что передача информации, осуществляемая с использованием новых информационных технологий, не должна нарушать прав и основных свобод человека, в частности права на неприкосновенность частной жизни и тайну переписки, как это гарантировано Статьей 8 Европейской конвенции о правах человека;

сознавая, что сбор, обработка и в особенности передача персональных данных с использованием новых информационных технологий по информационным магистралям регулируются положениями Конвенции о защите личности в отношении автоматизированной обработки персональных данных (Страсбург 1981, Серия европейских договоров N 108) и частными рекомендациями по защите данных, в особенности. Рекомендации N R (90) 19 о защите персональных данных, используемых при платежах и других смежных операциях. Рекомендацией N R (91) 10 о передаче третьим лицам персональных данных, находящихся в ведении государственных организаций, и Рекомендацией N R (95) 4 о защите персональных данных в области телекоммуникаций, в особенности в телефонии;

учитывая, что следует осведомить пользователей и поставщиков услуг Интернета об основных положениях упомянутой выше Конвенции при сборе и обработке персональных данных на информационных магистралях;

рекомендует правительствам государств-членов Совета Европы широко распространить приложение к данным рекомендациям, в особенности для пользователей и поставщиков услуг Интернета, а также для всех органов, ответственных за надзор за обеспечением защиты данных.

Приложение к Рекомендации N R (99) 5 Комитета Министров государствам-членам Совета Европы по защите неприкосновенности частной жизни в Интернете

Руководящие принципы по защите личности в отношении сбора и обработки персональных данных на информационных магистралях, которые могут быть включены или приложены в кодексы поведения

I. Введение

В данном документе изложены принципы обеспечения неприкосновенности частной жизни для Пользователей и Поставщиков услуг Интернета [1]. Эти принципы могут быть учтены в кодексах поведения.

Пользователи должны быть осведомлены об обязанностях Поставщиков услуг Интернета и наоборот. Поэтому целесообразно, чтобы Пользователи и Поставщики услуг прочитали весь этот документ, хотя для облегчения использования он разбит на несколько частей. К Вам может относиться одна или более частей данного руководства.

Использование Интернета накладывает ответственность на все Ваши действия и создает опасность для неприкосновенности частной жизни. Важно вести себя таким образом, чтобы обеспечить собственную защиту и поддерживать нормальные отношения с другими. Данный документ предлагает некоторые практические методы обеспечения неприкосновенности частной жизни, но Вам также следует знать Ваши права и обязанности, определенные законом.

Помните, что уважение неприкосновенности частной жизни - это основное право, которое должно быть защищено законом, в частности, законодательством по защите данных, и поэтому стоит уточнить Ваш юридический статус.

II. Пользователям

1. Помните, что Интернет - не безопасная сеть. Однако, существуют и разрабатываются различные средства, позволяющие повысить защиту ваших данных [2]. Поэтому, используйте все доступные средства для защиты Ваших данных и линий связи, как, например, легально доступные средства шифрования для конфиденциальной электронной почты, так и коды доступа к Вашему собственному персональному компьютеру [3].

2. Помните, что любая Ваша транзакция, любое посещение сайта в Интернете оставляет следы. Подобные "электронные следы" могут быть использованы без Вашего ведома, для создания профиля о Вас и ваших интересах. Если Вы не желаете такого сбора информации, то следует использовать новейшие технические достижения, позволяющие проинформировать Вас о любом случае возможности "следов", и отказаться от дальнейших действий. Также Вы можете запросить информацию о методах обеспечения неприкосновенности частной жизни, предоставляемых различными программами и сайтами, и предпочесть те из них, которые регистрируют минимум данных о пользователе или могут быть доступны анонимно.

3. Наилучший способ обеспечения неприкосновенности частной жизни - это анонимный доступ и анонимное использование услуг, анонимные средства осуществления платежей. Там, где это возможно, выясняйте наличие технических средств обеспечения анонимности [4].

4. Полная анонимность не всегда возможна в силу законодательных ограничений. В таком случае, если это разрешено законом, Вы можете использовать псевдоним, что позволит знать Ваши персональные данные только поставщику услуг Интернета.

5. Сообщайте вашему поставщику услуг Интернета или кому-либо только те данные, которые необходимы для выполнения определенных действий, о которых вы проинформированы. Особая осторожность необходима при использовании кредитных карт и номеров счетов, которые в Интернете могут легко стать объектом злоупотреблений.

6. Помните, что Ваш адрес электронной почты является информацией персонального характера и посторонние лица могут использовать его, например, для включения в справочники или списки пользователей. Не стесняйтесь спрашивать о назначении такого справочника. При желании Вы можете потребовать исключения данных о себе из подобных справочников и списков.

7. С осторожностью относитесь к сайтам, где у Вас просят информацию личного характера большую, чем это требуется для доступа или осуществления трансакции, или где не говорят, для чего такая информация необходима.

8. Помните, что Вы несете ответственность перед законом за обработку данных, например, если Вы незаконно загрузили или выгрузили данные. Все эти действия могут быть отслежены даже в случае использования Вами псевдонима.

9. Не рассылайте электронные почтовые сообщения злонамеренного содержания. Это может привести к преследованию по закону.

10. Ваш поставщик услуг Интернета несет ответственность за правильное использование персональных данных. Запросите Вашего поставщика услуг Интернета о том, как, с какой целью и какие данные о Вас он накапливает, обрабатывает и хранит. Периодически возобновляйте такой запрос. Настаивайте на изменении поставщиком Ваших данных, если они неправильны, или на удалении, если они избыточны, просрочены или больше не требуются. Требуйте, чтобы поставщик оповестил о такой модификации все стороны, которым ваши персональные данные передавались [5].

11. Если Вас не устраивает то, как Ваш поставщик услуг Интернет накапливает, использует, хранит и распространяет данные, и он при этом ничего не меняет, задумайтесь о смене поставщика услуг. Если Вы считаете, что поставщик не обеспечивает защиту персональных данных. Вы можете проинформировать компетентные органы или предпринять предусмотренные законом действия.

12. Старайтесь быть в курсе рисков неприкосновенности частной жизни и безопасности в Интернете и методов снижения таких рисков.

13. При отправке персональных данных в другую страну Вы должны учесть, что там они могут оказаться менее защищенными. В случае, если речь идет только о Ваших персональных данных. Вы вправе принимать любое решение. Однако, если Вы передаете не собственные персональные данные в другую страну. Вам следует запросить, например, компетентные органы, ответственные за защиту данных в Вашей стране, о том, допустима ли такая передача [6]. Вам следует потребовать принимающую сторону обеспечить меры [7], необходимые для обеспечения защиты персональных данных.

III. Поставщикам услуг Интернета

1. Используйте соответствующие процедуры и доступные технологии, предпочтительно сертифицированные, для обеспечения неприкосновенности частной жизни личности (даже если они не являются пользователями Интернета), в особенности путем обеспечения целостности и конфиденциальности наряду с обеспечением физической и логической безопасности сети и услуг, предоставляемых в сети.

2. Информируйте пользователей перед их подпиской на услуги или началом обслуживания о рисках неприкосновенности частной жизни при использовании Интернета. Подобные риски могут быть связаны с нарушением целостности данных, конфиденциальности, безопасности сети или со скрытым накоплением или сбором персональных данных.

3. Информируйте пользователя о технических средствах, которые он/она могут использовать на законном основании для снижения риска нарушения безопасности данных и их передачи, например, о разрешенных средствах шифрования и цифровой подписи. Предлагайте подобные технические средства на коммерческой основе, не злоупотребляя ценами.

4. Перед подпиской пользователей и предоставлением доступа в Интернет информируйте их о возможности анонимного доступа к сети с анонимной оплатой услуг (например, препейд карты доступа). В силу законодательных ограничений полная анонимность не всегда может быть возможна. В таком случае, если закон разрешает, предоставляйте возможность пользователю использовать псевдонимы. Информируйте пользователей о программных средствах анонимного поиска и просмотра информации в Интернете.

Проектируйте свою систему таким образом, чтобы избежать или минимизировать использование персональных данных.

5. Не читайте, не изменяйте или не удаляйте сообщения передаваемые другим лицам.

6. Не допускайте никакого вмешательства в содержимое передаваемых данных, если только это не предусмотрено законом и не осуществляется государственными органами.

7. Накапливайте, обрабатывайте и храните персональные данные пользователей только тогда, когда это необходимо для ясных, точно определенных и законных целей.

8. Не передавайте персональные данные, если такая передача не подкреплена законодательно [8].

9. Не храните персональные данные дольше, чем это необходимо для целей обработки [9].

10. Не используйте персональные данные для собственной рекламной или маркетинговой деятельности, если проинформированный о ваших намерениях пользователь возражает против этого или если в случае обработки передаваемых или специальных категорий данных, он/она не дал четкого согласия.

11. Вы отвечаете за надлежащее использование персональных данных. На Вашей вводной странице давайте ясную информацию о политике в части обеспечения неприкосновенности частной жизни. Эта информация должна иметь гиперссылку на детальное разъяснение такой политики. Прежде чем пользователь начнет пользоваться Вашими услугами, когда он/она посетит Ваш сайт или при любом его/ее запросе, проинформируйте его/ее о том, кто Вы, какие персональные данные Вы накапливаете, обрабатываете и храните, как вы это делаете, с какой целью и как долго Вы их храните. Если необходимо, запросите согласия пользователя. По запросу пользователя немедленно исправляйте его неверные данные и удаляйте их, если они избыточны, просрочены или больше не требуются, и прекращайте их обработку по требованию пользователя. Уведомляйте третью сторону, с которой Вы взаимодействуете, о любых модификациях. Избегайте скрытого сбора персональных данных.

12. Информация, предоставляемая пользователю, должна быть точной и актуальной.

13. Тщательно подумайте перед опубликованием персональных данных на вашем сайте! Подобная публикация может нарушить неприкосновенность частной жизни других людей и, кроме того, может быть запрещена законом.

14. Перед передачей данных в другую страну запросите, к примеру, компетентные органы Вашей страны, разрешена ли такая передача [10]. Вам следует просить принимающую сторону обеспечить необходимые меры защиты персональных данных.

IV. Пояснение и средства правовой защиты

1. Там, где в тексте используется термин "поставщик услуг Интернета", все сказанное применимо и к другим участникам Интернета, таким, как поставщики доступа (access providers), контент-провайдеры (content providers), поставщики сетевых услуг (network providers), разработчики программных средств навигации, операторы электронных досок объявлений и т.п.

2. Важна гарантия того, что Ваши права уважаются. Механизмы ответных действий, предлагаемые Группами пользователей Интернета (Internet user groups), Ассоциациями поставщиков услуг Интернета (Internet service provider association), органами власти, ответственными за защиту данных, или другими органами, являются чрезвычайно важными гарантиями выполнения данных рекомендаций. Установите контакт с упомянутыми организациями и органами в случае, если необходимы пояснения и средства правовой защиты.

3. Эти рекомендации распространяются на все типы информационных магистралей.

Примечания

1. - См. Главу IV, п.1

2. - Термин "данные" относится к "персональным данным" и означает любую информацию о Вас или о других лицах.

3. - Например, используйте пароли и регулярно изменяйте их.

4. - Например, при использовании Интернет-киосков, препейд карт доступа или платежных карт.

5. - Законы о защите данных, в соответствии со статьей 5 Конвенции Совета Европы о защите личности в отношении автоматизированной обработки персональных данных (СЕД N 108), должны предусматривать ответственность за точность и актуальность данных со стороны лица, осуществляющего их обработку.

6. - Законы многих европейских государств запрещают передачу данных в страны, где не обеспечен адекватный или эквивалентный уровень защиты. Однако, допускаются исключения, в частности, если субъект данных разрешил передачу его/ее данных в такую страну.

7. - Эти меры защиты могут быть разработаны и/или представлены в контракте на трансграничную передачу данных.

8. - В целом законы о защите данных разрешают передачу третьим лицам при определенных условиях, в частности

о специальных категориях данных и данных о графике, в случае если лицо, к которому они относятся, дало четкое согласие;

о других данных, там где их передача необходима для реализации законный целей или где лицо, к которому относятся данные, было проинформировано и дало не возражает.

9. - Например, не храните данные о счетах дольше, чем это необходимо по закону.

10. - См. примечание 6.

11. - См. примечание 7.