МОЛЧАНОВ С.В.,
кандидат юридических наук,
координатор региональных программ
Академического Международного института,
e-mail: mail@law-books.ru

ПРАВА ЧЕЛОВЕКА НА ДОСТУП К ЭЛЕКТРОННЫМ ИСТОЧНИКАМ ИНФОРМАЦИИ В СОВРЕМЕННЫХ РЕАЛИЯХ

АННОТАЦИЯ. Автор пишет о том, что вопрос о том, следует ли Интернет подвергать тотальному контролю, почти не рассматривался в отечественной и зарубежной науке. Исторически сложилось так, что Интернет ни в США, ни в Западной Европе никогда не был предметом государственного контроля. Чтобы установить связь с сетью «Интернет», не требуется лицензии. Сама сеть устроена так, что, имея к ней подсоединение, каждый получает возможность пользоваться большинством предоставляемых ею услуг. Иными словами, пользуясь одним и тем же подсоединением, можно предоставлять другим свои услуги в виде информации и подсоединения к различным источникам. Новые технологии размывают границы между содержанием информации и средством связи. В этом состоит отличие Интернета от всех прочих технологий связи и информации.

КЛЮЧЕВЫЕ СЛОВА: интернет, информация, информационная безопасность, средство связи, государственный контроль, закон.

MOLCHANOV S.V.,
Candidate of Law,
Coordinator of Regional Programs
of the Academic International Institute

HUMAN RIGHTS TO ACCESS ELECTRONIC SOURCES OF INFORMATION IN MODERN REALITIES

ANNOTATION. The author writes that the question of whether the Internet should be subjected to total control was almost not considered in domestic and foreign science. Historically, the Internet has never been subject to government control in the United States or Western Europe. You do not need a license to connect to the Internet. The network itself is arranged in such a way that, having a connection to it, everyone gets the opportunity to use most of the services provided by it. In other words, using the same connection, you can provide your services to others in the form of information and connection to different sources. New technologies blur the boundaries between the content of information and the means of communication. This is the difference between the Internet and all other communication and information technologies.

KEY WORDS: Internet, information, information security, means of communication, state control, law.

Вопрос о том, следует ли Интернет вообще подвергать тотальному контролю, почти не рассматривался, хотя в самом начале и были предприняты некоторые «вылазки» против сети. По мнению представителей большинства стран мира, Интернет как новая технология, никогда в прошлом не подвергавшаяся лицензированию или регулированию в смысле сферы услуг и тарифа оплаты, будет и в будущем развиваться вне государственного контроля, по мере того как более старые, ранее регулируемые технологии будут постепенно выходить из-под государственного контроля. И все же контроль над Интернетом – вещь не невозможная. В некоторых странах уже были предприняты меры для ограничения информации в Интернете [1].

В последние годы много внимания уделяется массовому мониторингу внутренних и международных коммуникаций со стороны спецслужб. По всему миру проводились расследования и парламентские слушания о координируемой Соединенными Штатами системе «Эшелон» [2].

Вскоре после окончания второй мировой войны, в 1947 г., правительства США, Великобритании, Канады, Австралии и Новой Зеландии подписали Пакт национальной безопасности, известный как «четырехстороннее» (Quadripartite) согла-

шение, или соглашение «Великобритания – США» (UKUSA). Его задачей было скрепить союз между разведками этих стран и обозначить общие цели по обеспечению национальной безопасности. Согласно условиям соглашения, пять стран-участниц разделили мир на пять зон влияния. Для каждой страны были определены приоритеты разведывательной работы.

Самый тесный союз в рамках UKUSA сложился между Агентством национальной безопасности США (NSA) и Главным управлением правительственной связи Великобритании (GCHQ). NSA действует в соответствии со специальной директивой 6 Совета национальной безопасности (NSCID) и прослушивает коммуникационные сети всего мира в разведывательных и военных целях. Со временем была создана громадная шпионская сеть, способная следить за телекоммуникационными системами любой страны. Эти операции настолько секретны, что подобная деятельность (за пределами США) осуществляется практически без законодательного или судебного надзора. Опорной точкой альянса является Менвис Хилл (Menwith Hill) – база королевских ВВС на севере Англии. Располагая более чем двумя десятками следящих станций и огромным количеством специального компьютерного оборудования, база способна прослушивать значительную часть коммуникаций. С появлением спутниковой и цифровой связи Менвис Хилл и ее аналоги в других странах получили возможность вести наблюдение и перехват в более широком масштабе [3].

В июле 2000 г. Европейский парламент создал специальную комиссию по «Эшелону», которая в мае 2001 г. представила свои выводы: «Существование глобальной системы перехвата коммуникаций… больше не вызывает сомнений» [4]. Согласно этим данным, система «Эшелон» (которой, как сказано в докладе, управляет США в сотрудничестве с Великобританией, Канадой, Австралией и Новой Зеландией) была создана в начале «холодной войны» в целях сбора разведданных, а в настоящее время превратилась в сеть станций перехвата по всему миру. Ее главная цель, считают авторы доклада, заключается в перехвате не военных, а частных и коммерческих сообщений.

Европейские эксперты рекомендовали гражданам и компаниям стран Евросоюза принять «меры самозащиты», а также поддержали дальнейшее развитие и использование в Европе криптографии для защиты коммуникаций от электронной слежки. Авторы доклада рекомендовали вынести на рассмотрение сессии Европарламента в Страсбурге в сентябре 2001 г. конкретные предложения. Эти предложения заключаются в следующем. Во-первых, США должны подписать соглашение с ЕС, по которому стороны обязаны соблюдать по отношению к другой стороне те положения о защите приватности граждан и тайне коммерческих коммуникаций, какие применяются по отношению к собственным гражданам и фирмам. Во-вторых, США должны подписать Международный пакт о гражданских и политических правах, чтобы частные лица могли обращаться с жалобами в Комитет по правам человека ООН. В-третьих, США должны принять кодекс этики, аналогичный тому, который действует в ЕС. Наконец, американцы должны начать диалог с Евросоюзом по поводу сбора экономических разведданных [5].

Эксперты также рекомендовали, чтобы Германия и Великобритания связали выдачу Соединенным Штатам разрешения на дальнейшие операции по перехвату коммуникаций на своей территории с условием соблюдением США Европейской Конвенции о правах человека. Ни одна из этих рекомендаций не была выполнена [6].

Эти события позволили наблюдателям прийти к двум выводам. Во-первых, до тех пор, пока американские, британские и прочие спецслужбы будут действовать вне эффективного парламентского и судебного контроля, их работа может быть направлена на ограничение и ущемление прав человека. По имеющимся данным, это уже происходит в отношении ряда организаций – Greenpeace, Christian Aid, Amnesty International, Международного комитета за запрещение противопехотных мин, правительства Тибета в изгнании, различных антиглобалистских движений, Independent Media Center, Комитета Красного креста.

Во-вторых, границы между спецслужбами и правоохранительными органами становятся все более условными. Если будет создана единая международная разведывательно-правоохранительная система электронной слежки, это будет означать, что запрет разведывательным службам вести слежку за гражданами собственных стран перестанет действовать.

В США контроль над содержанием информации разрешается согласно Первой поправке к конституции только в тех случаях, когда такой контроль оправдан в силу веского государственного интереса или применяется к очень узкому предмету [7]. Таким образом, контроль над содержанием информации в США – дело весьма непростое; исключение составляет контроль в целях ограждения от порнографии и защиты несовершеннолетних.

Государственный контроль над прессой и другими средствами массовой информации в США сводится к установлению баланса между

интересами свободы слова в чистом виде (включая конфиденциальный доступ к государственной документации) и неприкосновенностью частной жизни, интересами законопослушных граждан, малолетних и национальной безопасности.

Верховный суд США признал, что «обсуждение общественно значимых вопросов должно быть свободным, здоровым и открытым <…> даже включая страстные, язвительные и иногда неприятно резкие нападки на правительство и должностных лиц» [8]. В США регулированию, и то только в установленных конституцией рамках и после тщательного анализа, подлежат материалы, посягающие на чью-либо личную жизнь (включая те, что передаются при помощи компьютеров) или считающиеся непристойными (т.е. такие, которые вторгаются в частную жизнь законопослушных граждан или представляют угрозу для несовершеннолетних или для национальной безопасности).

В противовес этому, средства массовой информации, выполняя роль контролеров и оппозиционеров правительства, неизменно стремятся получить доступ к частным и государственным документам, а также проникнуть на заседания исполнительной, законодательной и судебной властей. Это их стремление отражено в федеральном законодательстве, например в законах о свободе информации и о защите конфиденциальных источников журналистов.

Проблемы, однако, неизбежно возникают в тех случаях, когда потребность прессы собирать и распространять информацию противоречит, например, конституционно гарантированным правам подзащитных по уголовным делам или способности прокуроров во имя защиты интересов государства возбуждать дело против обвиняемых. Возникающие при этом вопросы чрезвычайно сложны, а ответы подчас расплывчаты и неопределенны.

В Европе юридическая обстановка иная. В основе регулирования средств массовой информации здесь лежит запрет на высказывания, направленные на возбуждение ненависти. Действительно, ограничения в отношении такого рода высказываний были узаконены Международным пактом о гражданских и политических правах. Однако контроль, направленный на ограничение или запрещение возбуждающих ненависть высказываний, имеет свои проблемы. Не исключено, что определение такого рода высказываний будет столь широким, что многие виды высказываний или публикаций будут запрещены именно потому, что представляют угрозу сильным мира сего. С другой стороны, методы контроля над возбуждающими ненависть высказываниями (даже в очень узком смысле) могут быть таковы, что под запрет или ограничение попадут многие вполне законные высказывания.

Анализ Интернета, предпринятый специальным судом в более широком плане, применим к отношениям между новыми информационными технологиями и возможностью широкого воздействия на контроль над содержанием информации.

Заключение, к которому пришел суд, таково: благодаря свойствам Интернета, контролировать содержание передаваемой по нему информации (не подавляя при этом в значительной мере вполне законный обмен информацией) исключительно трудно, если вообще возможно [9].

Появление новых технологий побуждает страны принимать новое законодательство в области электронных коммуникаций. Принятие такого законодательства лоббируют правоохранительные органы и спецслужбы: им нужны более широкие возможности ведения электронной слежки [10].

Во всем мире признается, что прослушивание и электронная слежка – это следственные действия, которые грубо вторгаются в частную жизнь и которые должны применяться лишь в ограниченном числе нештатных ситуаций. Почти все крупные международные соглашения о правах человека защищают право людей не подвергаться несанкционированной, вторгающейся в частную жизнь слежке. Во многих странах мира приняты законы, ограничивающие перехват устных, телефонных, факсимильных и телексных коммуникаций. В большинстве демократических стран перехват коммуникаций может производиться правоохранительными органами и спецслужбами только после получения санкции судьи или иного независимого должностного лица высокого уровня и обычно лишь в связи с серьезными преступлениями. При этом часто требуется подтвердить, что иные следственные методы были испробованы, но не дали результата. Существуют различия в определении того, что такое «серьезные преступления» и что является должной санкцией.

В Японии прослушивание было разрешено как законный вид следственных действий лишь в 1999 г. Другие страны (Австралия, Германия, Новая Зеландия, Южная Африка и Великобритания) недавно внесли поправки в свое законодательство, которые облегчают слежку в условиях новых коммуникационных технологий [11].

Движение за усиление использования электронной слежки возглавило правительство США. Бывший Директор ФБР Луи Фри (Louis Freeh) исколесил мир, продвигая идею использования прослушивания в новых демократических странах, таких, как Венгрия и Чешская Республика.

Соединенные Штаты больше всех в мире приложили усилий, чтобы во все коммуникационные технологии закладывались возможности электронной слежки и чтобы было запрещено производить и использовать технологии, которые не поддавались бы мониторингу. Соединенные Штаты, кроме того, использовали свое влияние в международных организациях (Организация по экономическому сотрудничеству и развитию, «Большая восьмерка», Совет Европы), чтобы всячески содействовать распространению электронной слежки.

В ряде стран (Франция, Великобритания и др.) созданы специальные комиссии, которые вправе пересматривать условия проведения прослушивания и отслеживать злоупотребления. Такие комиссии наработали опыт, которым не обладают большинство санкционирующих слежку судей. Кроме того, комиссии имеют возможность проводить дополнительные проверки после завершения того или иного дела. В других странах определенными полномочиями по надзору за электронной слежкой обладают комиссии по защите приватности или по защите персональных данных [12].

Важной формой контроля во многих странах является требование того, чтобы государственные органы представляли ежегодный отчет об использовании электронной слежки. Такие отчеты обычно содержат краткие данные о числе случаев применения электронной слежки, о видах преступности, при расследовании которых она санкционировалась, о длительности ее применения и прочую информацию. Необходимость представлять отчеты – общая черта законодательства в области ограничения прослушивания в англоязычных и многих других странах, например в Австралии, Канаде, Франции, Новой Зеландии, Швеции, Великобритании и США [13].

Эти страны признают, что общество должно иметь право знать о применении электронной слежки, чтобы ограничить злоупотребления. Во многих странах отчеты используются контролирующими органами парламентов, журналистами, неправительственными группами и прочими организациями для проверки деятельности правоохранительных органов. Согласно отчетам, во многих странах, включая США и Великобританию, наблюдается рост использования электронной слежки, в то время как в других странах (например, в Канаде) этого не происходит [14].

Законы об ограничении прослушивания призваны гарантировать, чтобы законопослушные люди, например, журналисты, правозащитники, профсоюзные деятели, оппозиционные политики, не подвергались несанкционированной слежке только потому, что у них иные интересы и цели, чем у властных структур. Кроме того, такие законы призваны гарантировать, чтобы сравнительно мелкие правонарушения не были использованы как предлог для вторгающейся в частную жизнь электронной слежки, проводимой в политических или любых иных целях.

Во многих странах были обнаружены злоупотребления при проведении прослушиваний, и иногда в огромных масштабах. В результате страдали, как правило, те, кто доставлял неприятности властям: политические противники, студенческие лидеры, правозащитники [15]. Такое происходит даже в самых демократических странах. Например, в Швеции спецслужбы вели слежку за тысячами «левых» активистов в течение почти 40 лет.

Список литературы:

[1] Federal Communications Commission CC RM No. 8775; available from http://www.fcc.gov/Bureaus/Common_Carrier/WWW/hottopic.html#acta.

[2] Media Law Reporter 2553, 438 U.S. 726, 57 L. Ed. 2d 1073 (1978). 213 24 FCC2d 408 (1970).

[3] Американская ассоциация юристов. Правовая инициатива в Центральной и Восточной Европе. Современное право средств массовой информации в США. Центр права и средств массовой информации. Серия «Журналистика и право». Выпуск 8. http://www.internews.ru/books/modern/48.html.

[4] Руководящие принципы ОЭСР по безопасности информационных систем, приняты в ноябре 1992 г. (http://www.oecd.org).

[5] Плюрализм в электронных СМИ: роль технологий. Серия докладов. Институт Аспена и комиссия по политике радио и телевидения. 1995.

[6] О государственной защите нравственности и здоровья граждан и об усилении контроля за оборотом продукции сексуального характера: Проект ФЗ РФ // Справочно-правовая система «Гарант»

[7] ACLU v. Reno, 929 F. Supp. forthcoming.

[8] «Нью Йорк таймс Ко.» против Салливана (New York Times Co. v. Sullivan), 376 US 254, 279 (1964). С. 279).

[9] Bartow v. Smith, 149 Ohio Statute 301, 305, 78 N.E.2d 735 (Ohio 1948).

[10] Фатьянов А.А. Тайна и право (основные системы ограничений на доступ к информации в российском праве). М., 1999.

[11] Кертли Д. Свобода информации должна служить всему обществу, а не только журналистам // Российская журналистика: свобода доступа к информации. М., 1996. С. 207.

[12] Вершинин М.С. Политическая коммуникация в информационном обществе. СПб., 2001. С. 115, Волчинская Е.К., Терещенко Л.К., Якушев М.В. Интернет и гласность. М., 1999. С. 27.

[13] Information Society: Challenges for Politics, Economy and Society / http:www.bmwi-info2000.de/gip/fakten/zvei_e/index.html.

[14] Американская ассоциация юристов. Правовая инициатива в Центральной и Восточной Европе. Современное право средств массовой информации в США. Центр права и средств массовой информации. Серия «Журналистика и право». Выпуск 8 // http://www.internews.ru/books/modern/48.html.

[15] Государственный департамент США. Доклад о ситуации с правами человека за 1997 год, 30 января 1998 г. // www.hro.org/docs/reps/privacy/phr2002/phr2002_15.php?printv=1.

Spisok literatury:

[1] Federal Communications Commission CC RM No. 8775; available from http://www.fcc.gov/Bureaus/Common_Carrier/WWW/hottopic.html#acta.

[2] Media Law Reporter 2553, 438 U.S. 726, 57 L. Ed. 2d 1073 (1978). 213 24 FCC2d 408 (1970).

[3] American Bar Association. Legal initiative in Central and Eastern Europe. Modern media law in the United States. Center for Law and Media. "Journalism and Law" series. Issue 8. http://www.internews.ru/books/modern/48.html.

[4] OECD Guidelines on Information Systems Security, adopted in November 1992 (http://www.oecd.org).

[5] Pluralism in electronic media: the role of technology. Series of reports. Aspen Institute and Radio and Television Policy Commission. 1995.

[6] On state protection of morality and health of citizens and on strengthening control over the circulation of sexual products: Draft Federal Law of the Russian Federation//Reference and legal system "Garant"

[7] ACLU v. Reno, 929 F. Supp. forthcoming.

[8] "New York Times Co. v. Sullivan," 376 US 254, 279 (1964). S. 279).

[9] Bartow v. Smith, 149 Ohio Statute 301, 305, 78 N.E.2d 735 (Ohio 1948).

[10] Fatyanov A.A. Mystery and law (the main systems of restrictions on access to information in Russian law). M., 1999.

[11] Kurtley D. Freedom of information should serve the whole society, not just journalists//Russian journalism: freedom of access to information. M., 1996. S. 207.

[12] Vershinin M.S. Political communication in the information society. St. Petersburg, 2001. S. 115, Volchinskaya E.K., Tereshchenko L.K., Yakushev M.V. Internet and publicity. M., 1999. S. 27.

[13] Information Society: Challenges for Politics, Economy and Society / http:www.bmwi-info2000.de/gip/fakten/zvei_e/index.html.

[14] American Bar Association. Legal initiative in Central and Eastern Europe. Modern media law in the United States. Center for Law and Media. "Journalism and Law" series. Issue 8// http://www.internews.ru/books/modern/48.html.

[15] U.S. State Department. Human Rights Report 1997, 30 January 1998// www.hro.org/docs/reps/privacy/phr2002/phr2002_15.php?printv=1.