**Двадцать первый век и проблемы информационной безопасности в России**

Каландаров Камилжан Хамидович доктор философских наук, Генеральный директор Института прав человека

Кто сегодня будет спорить с утверждением, что на пороге двадцать первого века информация является главным фактором управления современным миром и основным ресурсом и инструментом власти? Справедливы слова: "кто владеет информацией, тот владеет миром". Государство может добиться стратегических преимуществ, лишь когда оно обладает полноценными информационными возможностями. Мы считаем, что безопасность нашей страны во многом зависит от эффективного функционирования информационной среды. Пожар в Останкино поставил остро вопрос об уязвимости системы информационной безопасности в Российской Федерации: столица и ее регион остались без телевидения и систем связи, что, во-первых, нарушает право жителей Москвы на информацию, во-вторых, ставит в максимально незащищенное положение саму федеральную власть. Эти события наглядно продемонстрировали неспособность нашей государственной власти справиться в полном объеме с задачей обеспечения безопасности всех субъектов информационных отношений. Сегодня в соответствии с законом она отвечает лишь за вопросы защиты государственной тайны, в большинстве же остальных случаев при неопределенности роли государственного участия бремя обеспечения информационной безопасности ложится на плечи граждан и общества, хотя это и отвечает конституционному принципу самозащиты своих интересов всеми способами, не запрещенными законом, однако такой подход лишает граждан и организации уверенности в завтрашнем дне, препятствует привлечению инвестиций на эти цели, что в итоге не позволяет решать проблемы.

Для обеспечения информационной безопасности, прежде всего, необходима система законодательных актов и созданных на их основе структур и механизмов взаимодействия по защите интересов субъектов правоотношений. При этом ее устойчивость должна основываться на общенациональном согласии. Решение этой проблемы важно для современной России, так как информационная безопасность является одной из основных составляющих системы обеспечения национальной безопасности в целом, более того, она во многом определяет в современных условиях ее успешное функционирование (Урсул А.Д. Информационное общество. Введение в социальную информатику. - М., 1990).Что необходимо для построения безопасного гражданского общества в России? Думается, реализация следующих задач:

переход от идеологического общества к информационному;

научное прогнозирование и моделирование решения возникающих проблем на альтернативной основе;

законодательное регулирование и защита информационной деятельности при обеспечении достоверности, открытости и свободы информации;

освобождение сознания людей от стереотипов тоталитаризма и прекращение психологической войны политического руководства против народа в любых формах ее проявления. Эти положения закреплены в Законе РФ "О безопасности", других федеральных законах, однако, к сожалению, до сих пор конкретных результатов нет. В современной России существует целый комплекс проблем, без решения которых невозможно сдвинуть дело с мертвой точки. Что это за проблемы? Это, прежде всего: - отсутствие единой системы отбора информации, подготовки и принятия решений на высшем уровне;

отсутствие должного взаимодействия между существующими структурами обеспечения безопасности, когда ведомства порой подменяют государственные интересы узковедомственными и вступают в противостояние за усиление своих полномочий;

отсутствие системы эффективного контроля за обеспечением безопасности как со стороны вышестоящих государственных структур, так и со стороны общества и граждан, в силу чего нередко даже правильные и необходимые решения не выполняются.

Итак, Россия сегодня стоит перед необходимостью совершенствования системы обеспечения безопасности, в том числе в информационной сфере, и это не голословное утверждение (Урсул А.Д. Переход России к устойчивому развитию: ноосферная стратегия. - М., 1998).

Информационная безопасность основывается на свободе информации и запретительном принципе права (все, что не запрещено законом, - разрешено). Это закреплено в основных международных правовых документах, Конституции РФ и ряде федеральных законов.

Существуют четко сформулированные ограничения на свободу слова. Конституция РФ в ч. 3 ст. 17 и ч. 3 ст. 55 к основаниям ограничения основных информационных прав и свобод гражданина относит следующие: защита основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечение обороны страны и безопасности государства. Кроме того, ст. 56 предусматривает возможность ограничения прав и свобод с указанием пределов и сроков их действия в условиях чрезвычайного положения в соответствии с федеральным конституционным законом. К прямым ограничениям прав и свобод Конституция относит (ч. 1 и 2 ст. 23; ч. 1 ст. 24, ч. 2 и 4 ст. 29) все случаи, предусмотренные "Декларацией прав и свобод человека и гражданина". Дополнительно введены ограничения на использование информационных прав и свобод с целью пропаганды социальной ненависти, социального, расового, национального и религиозного или языкового превосходства.

Что необходимо предпринять?

Руководствуясь принципом приоритета норм международного права над национальным законодательством, следует подготовить унифицированный перечень оснований для ограничений прав и свобод с последующим внесением изменений в Конституцию РФ и международные акты.

Во всех рассмотренных документах прямо указывается, что ограничения информационных прав и свобод могут быть установлены только законом, при этом не предусматривается разрешительный принцип реализации указанных прав и свобод. Все основания для ограничений можно свести к трем группам: для защиты интересов личности, обеспечения стабильности в обществе, а также в интересах обороны и безопасности государства.

Анализ действующего законодательства в сфере информационной безопасности (более 80 законов) выявил принципиальные недостатки законодательной базы: противоречивость, декларативность, наличие "белых пятен", неточность понятийного аппарата.

В законодательстве сегодня упоминается более 30 видов тайн, которые выступают в виде прямых ограничений для реализации информационных прав и свобод. В последние годы предпринималось несколько попыток их упорядочивания. Так, в ФЗ "Об информации, информатизации и защите информации" (ст. 8 и 10) 1995 г. вся информация с ограниченным доступом подразделяется на государственную тайну и конфиденциальную информацию. При этом из многочисленных видов конфиденциальной информации в законе упомянуты лишь личная, семейная тайны, персональные данные, тайна переписки, телефонных, почтовых, телеграфных и иных сообщений. Но уже в ФЗ "Об участии в международном информационном обмене" (ст. 8) 1996 г. государственная тайна определяется как один из видов конфиденциальной информации. Эта путаница сохраняется во многих законах, где ссылки "на иные охраняемые секреты", "иные охраняемые законом тайны" предполагают продолжение списка видов информации с ограниченным доступом.

Понятие конфиденциальной информации обычно определяется как информация, "не являющаяся общедоступной и могущая нанести ущерб правам и охраняемым законом интересам предоставившего ее лица". Но уже в законе "Об информации, информатизации и защите информации" (ст. 2) и законе "Об участии в международном информационном обмене" (ст. 2) конфиденциальная информация определена как "документированная информация, доступ к которой ограничивается законодательством РФ". Это приводит к произвольному толкованию исходных понятий и затрудняет реализацию законов.

Очевидно, для упорядочения работы с конфиденциальной информацией необходимо законодательно закрепить единый перечень видов такой информации с определением их соотношения, установления ответственности за нарушение режима ограничения доступа к ней, а также механизмы изменения режимов ограниченного доступа (в том числе замену одного режима другим). Можно предложить следующий перечень видов информации с ограниченным доступом:

государственная тайна;

конфиденциальная информация: неприкосновенность частной жизни, коммерческая тайна, профессиональная тайна, служебная тайна.

Правовое регулирование отношений в каждом из этих случаев должно быть закреплено отдельным законом. И чем скорее это произойдет, тем более успешно можно будет реализовать основные информационные права граждан и защищать интересы общества и государства.

В Конституции РФ заложены основания, по которым отдельные виды информации не подлежат какому-либо ограничению, например, в ст. 42 указано право на достоверную информацию о состоянии окружающей среды, которое не может быть ограничено. В случае если это состояние угрожает жизни и здоровью людей, должностные лица обязаны информировать население об этом, в противном случае наступает юридическая ответственность.

В ряде законов, устанавливающих ограничения доступа к информации, также вводится перечень сведений, доступ к которым не может быть ограничен. Так, в ст. 7 Закона "О государственной тайне" перечислены сведения, не подлежащие засекречиванию.

В п. 3 ст. 10 Закона "Об информации, информатизации и защите информации" приведен список документированной информации, доступ к которой запрещено ограничивать. В Законе "О коммерческой тайне" планируется также установить перечень сведений, которые нельзя относить к коммерческой тайне. В законе "О благотворительной деятельности и благотворительных организациях" (п. 7 ст. 19), в свою очередь, определен перечень сведений, которые не могут составлять коммерческую тайну.

В Положении о порядке обращения со служебной информацией ограниченного распространения, утвержденном Постановлением Правительства РФ № 1233 от 03.11.94, также установлен перечень сведений, которые не могут быть отнесены к такой информации. Это создает опасность замены запретительного принципа права, закрепленного в международных документах и Конституции РФ, разрешительным, когда основные информационные права и свободы можно будет реализовать только в установленных чиновником случаях.

Конституция РФ устанавливает, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. В то же время, в интересах борьбы с преступностью и безопасности государства могут быть проведены на законном основании оперативно-розыскные мероприятия в отношении отдельных лиц, предусматривающие сбор, хранение и использование информации об их частной жизни без их согласия.

Перечень оснований и случаев их использования должен быть исчерпывающим и установлен законом. Причем даже в этом случае в законах должны быть заложены механизмы защиты прав гражданина на неприкосновенность частной жизни. В нынешних законах, регулирующих оперативно-розыскную деятельность (ОРД) правоохранительных органов, сформулированы такие основные правила:

право обжаловать неправомерные действия конкретного должностного лица в структуре, осуществляющей ОРД, вышестоящему должностному лицу, в суд или прокуратуру;

право лица на получение информации, собранной в отношении его, если не доказано судом преступление, задуманное или совершенное этим лицом, и обязанность должностных лиц предоставить такую информацию;

обязанность должностных лиц структур, осуществляющих ОРД, а также судов и прокуратуры восстановить конституционное право граждан в случае незаконного вмешательства в их частную жизнь.

Для исполнения этих правил необходимо их закрепление во всех законах, касающихся возможности сбора информации о частной жизни, в том числе, в Законе "О средствах массовой информации" (ст. 4, 51, 57); определить механизмы установления ответственности должностных лиц и журналистов, превысивших свои полномочия (требует существенного уточнения и сокращения перечня случаев освобождения журналистов от ответственности за распространение информации о частной жизни лица), а также механизмы восстановления конституционных прав граждан.

Несмотря на заявленные в Конституции РФ права на информацию и предусмотренную УК РФ ответственность за непредоставление информации гражданам, палатам Федерального Собрания РФ и Счетной палате РФ (ст. 140 и 287), реализации этих прав во многом препятствует декларативность законов и отсутствие механизмов доступа к открытой информации.

Так, в действующих законах предусмотрена ответственность за следующие виды нарушений указанных прав: непредоставление сведений, несвоевременное предоставление сведений, сокрытие информации, сообщение ложных (недостоверных) сведений, ограничение права на предоставление информации, искажение сведений, нарушение свободного международного информационного обмена. Требуется унификация по видам заявленных в законах правонарушений в этой области с прописыванием механизмов установления ответственности в соответствующих кодексах.

К механизмам доступа к открытой информации можно отнести:

обязанность должностных лиц на основе документов предоставлять по запросам граждан информацию, доступ к которой не ограничен законом;

публикацию в общедоступных изданиях перечней оснований и случаев установления ограничений основных информационных прав и свобод, видов конфиденциальной информации; сведений, доступ к которым не может быть ограничен;

порядок предоставления такой информации, предусматривающий сроки, объем и форму предоставления информации в зависимости от правового статуса организации, в адрес которой направлен запрос;

создание общедоступных баз данных в органах государственной власти и местного самоуправления, в том числе на общедоступных серверах с указанием в средствах массовой информации их адресов и порядка получения информации.

Особое место среди перечисленных видов информации занимает информация, которая не может быть отнесена к конфиденциальной и, в то же время, она требует ограничения своего распространения в силу ее негативного влияния на нравственное состояние общества (в том числе информация, возбуждающая социальную, расовую, национальную или религиозную ненависть и вражду, пропаганда превосходства, распространение порнографии и др.), посягательства на честь, доброе имя и деловую репутацию, а также на здоровье людей. Примером последнего может служить недобросовестная реклама; вредное влияние, неосознаваемое человеком, на его подсознание со стороны других людей с парапсихологическими способностями, оккультных организаций, через средства массовой информации с использованием специальных технологий (25-й кадр) и путем применения специальной техники (так называемые пси-генераторы).

Указанные ограничения отчасти закреплены в Конституции РФ, но законодательно не установлены критерии выявления такой информации и проведения экспертизы, а также механизмы реализации ограничений (режим распространения). Это существенно затрудняет установление фактов нарушений и привлечение к ответственности виновных лиц, хотя в некоторых законах такая ответственность декларируется ("за использование скрытой рекламы", "нарушение требований к рекламе отдельных видов товаров", "использование информации во вред себе и другим", "за клевету и оскорбление", "за публичные призывы к развязыванию агрессивной войны").

Это подтверждает актуальность подготовки законопроектов по вопросам обеспечения информационно-психологической безопасности, запрещения пропаганды ненависти, вражды и превосходства (в том числе фашизма), а также установления ответственности за подобные правонарушения.

Очевидно, что продолжение прежней практики законотворчества без единой концепции законодательства в информационной сфере блокирует реализацию конституционных прав граждан, делает трудновыполнимой задачу построения правового государства и информационного общества в России. Такая концепция должна быть направлена на регулирование правоотношений, возникающих при реализации основных информационных прав по основным видам информации и могла бы основываться на изложенных выше положениях. При этом в каждом случае важно установить права, обязанности и ответственность субъектов правоотношений.

Исходя из предложенного понимания безопасности в информационной сфере и в соответствии с данной концепцией в законодательстве должны быть предусмотрены:

защита прав на получение информации (достоверной, полной и оперативной) и на ограничение доступа к информации;

защита информации от искажения;

защита пользователя от недостоверной, ложной и вредной информации;

защита информационных систем.

Исходя из этого, государственная политика должна через федеральные программы определить решение следующих задач:

оценка состояния существующих информационных систем и научно-промышленного, кадрового потенциала для развития этих систем и средств их защиты;

экспертиза и классификация по степени защищенности основных видов систем;

определение возможностей и условий интеграции информационных систем, в том числе в регионах России, на федеральном уровне, между федеральным центром и субъектами РФ, в СНГ и между государствами - членами Совета Европы;

определение количественных и качественных параметров развития информационных систем на ближайшие годы;

определение общей потребности в инвестициях, масштабов и форм государственного участия (в том числе создание льготных условий для привлечения негосударственных инвестиций в эту сферу);

унификация законодательства на межгосударственном уровне на основе системы модельных законов и с учетом "Иоганнесбургских принципов", принятых группой экспертов в области международного права 01.10.95.

Необходимо законодательное закрепление полномочий органов государственной власти и госструктур в единой системе обеспечения безопасности информационных систем. Для этого целесообразно принятие специального закона "О защите информации и противодействии иностранным техническим разведкам", а также внесение изменений в законы "О связи", "Об информации, информатизации и защите информации".

Особое место в законодательстве должны занимать правоотношения, возникающие в процессе использования компьютерных систем и сетей. Специфика правонарушений в этой сфере частично нашла отражение в главе 28 УК РФ (ст. 272-274), однако из-за нечеткости формулировок, отсутствия механизмов расследования таких преступлений и подготовленных кадров, достаточной технической базы и правоприменительной практики эти статьи УК РФ невыполнимы в ближайшее время.

Вот почему органы государственной власти должны четко определить свой интерес, исходя из реальных возможностей и заявленных приоритетов в обеспечении безопасности.

Одновременно с этим целью государственной политики должно стать создание условий для максимально быстрого роста негосударственного компонента системы информационной безопасности на основе объединения усилий отдельных субъектов и установления диалога и эффективного взаимодействия с ними со стороны государства.

Только при условии понимания государством в лице органов власти своих интересов, формулирования, заявления и реализации единой государственной политики, обеспечения понимания этой политики в обществе и организации взаимодействия со всеми структурами гражданского общества и действенного контроля с их стороны возможно создать как информационное общество, так и правовое государство в России.