«ДОСТАТОЧНО ОСОЗНАВАТЬ, ЧТО ОНА ЕСТЬ»

гражданское общество, секретность и слежка в Беларуси

AMNESTY INTERNATIONAL

Amnesty International – всемирное движение, которое насчитывает более 7 миллионов человек, борющихся за мир, в котором права человека доступны каждому.

Мы стремимся к тому, чтобы каждый человек мог пользоваться всеми правами, провозглашёнными во Всеобщей декларации прав человека и других международных стандартах в области прав человека.

Мы не зависим ни от каких правительств, политической идеологии, экономических интересов или религиозных воззрений, и получаем основную часть средств за счёт членских взносов и добровольных пожертвований.

Впервые опубликовано в 2016 году
Amnesty International Ltd
Peter Benenson House, 1 Easton Street
London WC1X 0DW, UK

Индекс: EUR 49/4306/2016
Язык оригинала: Английский

amnesty.org

***Фото на обложке:** Минск, Беларусь*
© Максим Сарьнев

AMNESTY INTERNATIONAL

ОГЛАВЛЕНИЕ

СЛОВАРЬ

IP-адрес	**УНИКАЛЬНЫЙ АДРЕС УЗЛА В ИНТЕРНЕТЕ ИЛИ ЛОКАЛЬНОЙ СЕТИ.**
IMEI-номер	Международный идентификатор мобильного оборудования: номер, который используется для определения мобильного телефона.
IMSI-номер	Международный идентификатор мобильного абонента: номер, который используется для определения мобильного абонента.
MAC-адрес	Уникальный идентификатор аппаратного обеспечения, который присваивается сетевому адаптеру компьютера при изготовлении.
метаданные	Данные, которые используются при сетевой коммуникации, не являясь её содержанием. Например (но не только): отправитель и получатель сообщений, время коммуникаций, местонахождение отправителя или получателя.
прокси-сервер	Сервер, который используется в качестве посредника при запросах клиентов к другим серверам (обычно веб-серверам). Прокси-сервер может использоваться для записи или изменения содержания веб-сайтов, запрошенных через него.
VPN	Виртуальная частная сеть: технология, которая используется при создании безопасного, шифрованного соединения между компьютерами в небезопасной сети общего пользования (например, в интернете).

КГБ	Комитет государственной безопасности Республики Беларусь, национальное разведывательное агентство.
ОМОН	Отряд милиции особого назначения.
ОАЦ	Оперативно-аналитический центр при президенте, агентство, которое отвечает за защиту информации и охрану государственных тайн; играет в Беларуси важную роль в регулировании вопросов, связанных с интернетом, в том числе вопросов, связанных со слежкой.

1. КРАТКОЕ СОДЕРЖАНИЕ

Правовая база, регулирующая порядок негласного наблюдения в Беларуси, характеризуется отсутствием соответствующих гарантий безопасности, и позволяет властям осуществлять широкомасштабную слежку практически без всякого обоснования. И хотя фактически любой человек может стать объектом слежки, почти невозможно узнать, ведётся ли за ним слежка сейчас, или она велась ранее. Подобная неопределённость оказывает сковывающий эффект на правозащитников, оппозиционных политиков, юристов и активистов, и ограничивает их возможности в реализации своих прав, в том числе права на неприкосновенность частной жизни, свободу объединений, свободу мирных собраний и свободу выражения мнений.

И хотя негласное наблюдение может являться законным инструментом в работе правоохранительных органов, - в отсутствие надлежащих гарантий безопасности, надзора или в случае иных отступлений от международного права и стандартов, оно нарушает права человека. В настоящем докладе рассматриваются аспекты, в которых незаконная тайная слежка затрагивает права человека, а также тот эффект, который она оказывает на гражданское общество в Беларуси. Доклад основывается на интервью с более чем пятьюдесятью активистами гражданского общества; в основном интервью проходили в Беларуси, но также и в других странах. Кроме того, доклад основан на детальном изучении белорусской и международной законодательной базы, определяющей порядок ведения слежки.

У системы слежки в Беларуси много проблемных аспектов. В их ряду особое место занимает система «СОРМ», набор стандартизированных технических средств для перехвата коммуникаций, позволяющих властям удалённо получать прямой доступ ко всем коммуникациям пользователей и связанной с ними информации, не уведомляя об этом провайдеров. В соответствии с белорусским законодательством, все телекоммуникационные провайдеры в стране обязаны обеспечивать совместимость своего оборудования с системой «СОРМ». Эта система обеспечивает мониторинг коммуникаций в режиме реального времени, а также доступ к данным, которые телекоммуникационные компании по закону обязаны сохранять на срок до пяти лет. Это обеспечивает доступ как к содержанию коммуникаций, так и к связанным с ними метаданным (таким, как время, характер или место коммуникации).

Этой противоречивое системе слежения оказывают содействие корпоративные игроки, такие как операторы мобильной связи и интернет-провайдеры, которые – в соответствии с белорусским законодательством – обязаны предоставлять властям прямой доступ к данным своих клиентов. Эти белорусские компании, а также международные компании, являющиеся их владельцами или основными акционерами, оказываются не в состоянии (в нарушение своих обязательств) определить, предотвратить и остановить нарушения прав человека, происходящие в результате их деятельности или вытекающие из их хозяйственных отношений. Таким образом, они причастны к нарушению международных стандартов ведения бизнеса и международных стандартов в области прав человека. Компании должны предпринимать конструктивные шаги для выполнения своих обязательств в области прав человека, независимо от того, где они решили осуществлять свою деятельность. Эти шаги должны быть соизмеримы с угрозой ущерба, с которым люди сталкиваются в результате их действий.

Слежка за телекоммуникациями – не единственная угроза слежки, с которой сталкиваются белорусы. Право на неприкосновенность частной жизни также оказывается под угрозой, так как законодательство предоставляет широкие полномочия для физической слежки, в том числе прослушивания людей или помещений, а также в связи с тем, что неприкосновенность личной информации может пострадать, когда власти конфискуют компьютеры, мобильные телефоны или другие устройства. Отсутствие прозрачности в отношении возможностей государства осуществлять слежку означает, в конечном итоге, что никто не знает всего комплекса средств и технологий, имеющихся в распоряжении властей.

Тайное наблюдение осуществляется многочисленными государственными службами, чьи полномочия основываются на большом количестве расширительных и неопределённых юридических оснований. В соответствии с национальным законодательством оно может применяться, для того, чтобы установить слежку за людьми, которые не подозреваются в каких-либо противоправных деяниях. Предоставление полномочий и гарантии безопасности в отношении надзора не являются достаточными; обычно надзор осуществляют прокуроры, а не независимый судебный орган.

Когда слежка приводит к нарушениям прав человека, получить правовую защиту на практике оказывается крайне трудно. В особенности это справедливо, поскольку власти не обязаны извещать объекты слежки о том, что за ними велась слежка, после её окончания – даже если такое уведомление могло быть предоставлено без ущерба для целей расследований. Как следствие, люди редко получают доступ к доказательствам, которые могли бы подкрепить их жалобу. Почти никто из активистов, уверенных, что за ними велась незаконная слежка, не смогли обратиться с жалобой. Из тех же, кто подал жалобу, почти никто не верил, что их жалобы приведут к какому-нибудь результату, и зачастую подавали их лишь для того, чтобы самим не стать объектом судебного преследования.

Существующая в Беларуси законодательная база делает почти невозможным для кого-либо выяснить точно, мог ли он быть объектом слежки – сейчас или в прошлом; при этом новейшая белорусская история даёт многим активистам основания полагать, что слежка за ними ведётся.

Репрессии со стороны властей, последовавшие за президентскими выборами 2010 года, выразились в арестах и тюремных заключениях членов политической оппозиции за попытку реализовать свои права. Характерной чертой многих из этих судебных процессов, получивших широкое освещение в прессе, было регулярное привлечение информации из личных коммуникаций и связанных с ними данных; многие СМИ сообщали, что данные о местоположении мобильного телефона использовались властями для того, чтобы определять личности участников неразрешённых – но носивших в основном мирный характер – демонстраций, последовавших за выборами.

Отчасти по этой причине активисты, которые говорили с Amnesty International, все как один выражали уверенность в том, что за ними в той или иной форме велась слежка из-за их деятельности. Этот страх слежки обостряется ограничительным характером правовой среды, в которой существует гражданское общество в Беларуси; активисты постоянно подвергаются наказаниям исключительно за реализацию своих прав – таких, как участие в мирном протесте, – а также сталкиваются со всё более жёсткими ограничениями в реализации прав человека в интернете. Всё это оказывает сковывающий эффект, который заставил многих прибегать к самоцензуре и воздерживаться во многих случаях от реализации своих прав.

Активисты, с которыми Amnesty International проводила интервью, заявили, что обычно они не обсуждают щекотливые темы по телефону, – например, вопросы финансирования незарегистрированной организации или организацию мирного протеста - и то, и другое может привести к уголовным обвинениям. Даже такие будничные организационные вопросы, как, например, организация встречи, предполагают использование сложного кодированного языка; и как правило, требуется личная встреча, часто на открытом воздухе, без мобильных телефонов, которые могли бы записывать их разговоры или отслеживать их местоположение. Кроме того, опасения по поводу слежки за цифровыми коммуникациями делают использование средств шифрования, в том числе PGP (системы шифрования электронной почты), закодированных программ чатов и шифрование диска, неотъемлемой частью работы активистов.

Активисты сообщали о ситуациях (например, их остановила милиция, которая, казалось, знала, где их найти), которые они приписывали отслеживанию местонахождения их мобильных телефонов. Учитывая, однако, проблемы действующей в Беларуси законодательной базы, они не могут подтвердить подобные подозрения, и у большинства людей не остаётся других вариантов, кроме как предположить, что их местоположение отслеживается.

Некоторые активисты опасались, что в их офисах или даже в их домах может вестись прослушивание или видеонаблюдение, что не давало им решать деликатные рабочие вопросы на своих собственных рабочих местах; это существенно ограничивало их способность заниматься своей работой.

Amnesty International разговаривала с тремя активистами, которые заявили, что они уверены, что их электронная почта или аккаунты в социальных сетях были взломаны. Они подозревали, что за этими атаками могут стоять власти, и эти подозрения, по их словам, усилились после того, как их личные данные были использованы для их запугивания или преследования. Чаще случалось, что власти конфисковывали компьютеры или другое оборудование активистов, в результате чего те не могли продолжать работать на этом оборудовании даже после того, как его возвращали, так как опасались, что на нём может быть установлено программное обеспечение, позволяющее осуществлять слежку.

Использование интернета в Беларуси за последние годы резко возросло. В 2014 году уровень доступа к интернету составил 59% против 39.6% в 2011 году.[1] Несмотря на это, неопределённость и угроза возможной слежки за коммуникациями затрудняет работу белорусских активистов. Активисты не могут воспользоваться преимуществами улучшившихся возможностей взаимодействия. Вместо этого из-за сковывающего эффекта, вызванного опасением по поводу слежки, коммуникации замедляются, поток информации ограничивается, организационная активность затухает и подрывается взаимное доверие.

Из-за проблем в законодательной базе, регулирующей порядок слежки в Беларуси, каждый вынужден жить так, как если за ним ведётся скрытое наблюдение, что негативно сказывается на соблюдении прав человека. В то время как сегодня невозможно установить существующий масштаб слежки, воздействие имевших место в прошлом злоупотреблений очевидны: в прессе широко освещались случаи, когда власти использовали данные о коммуникациях для судебного преследования оппозиционных политиков и правозащитников после выборов 2010 года; эти случаи по-прежнему называют главной причиной того, что люди опасаются слежки. Случаи, описанные активистами, говорившими с Amnesty International, показывают, что они по-прежнему остаются объектами негласного наблюдения.

Белорусские власти должны незамедлительно пересмотреть законы, регулирующие использование тайного наблюдения, чтобы привести их в соответствие с международными стандартами. Например, они должны обеспечить, чтобы слежка применялась только с санкции (и под надзором) независимых судей и при наличии чётко определённых оснований, принимая во внимание необходимость индивидуализированных обоснованных подозрений в противоправной деятельности и требования необходимости и соразмерности. Систему «СОРМ» должна сменить такая система, которая не обеспечивает прямой доступ к данным о коммуникациях. Прокуроры не должны подвергать людей слежке за реализацию их прав, таких как организация мирных протестов. Прокуроры и власти, осуществляющие слежку, должны с большей готовностью предоставлять информацию о количестве случаев санкционирования и ведения слежки. Люди, ставшие объектом слежки, должны получать соответствующее уведомление, и иметь эффективный доступ к средствам правовой защиты от нарушений прав человека, связанных со слежкой. Частные компании, способствующие осуществлению слежки в Беларуси, должны оспаривать незаконную правительственную практику слежки, добиваться её реформирования и быть более прозрачными в отношении законодательства и практики, определяющих доступ к данным пользователей в Беларуси.

Дополнительные рекомендации содержатся в конце этого доклада.

[1] http://data.worldbank.org/indicator/IT.NET.USER.P2

2. МЕТОДОЛОГИЯ

Данный доклад основан на интервью с более чем пятьюдесятью активистами, правозащитниками, журналистами, юристами, оппозиционерами, экспертами в области технологий и другими лицами, многие из которых живут в изгнании. По большей части интервью проводились в Минске (Беларусь), другие проходили в Вильнюсе (Литва) и Варшаве (Польша) в период с августа по декабрь 2015 года. Дополнительные интервью проводились – как удалённо, так и при личной встрече - в Лондоне в течение 2016 года. Во многих случаях имена тех, кто давал интервью, а также некоторые другие личные данные, были опущены или изменены для того, чтобы сохранить анонимность источников.

Amnesty отправила краткое изложение полученных сведений и вопросов, вызывающих обеспокоенность, и пыталась получить информацию и комментарии у большого числа правительственных организаций, в том числе в обеих палатах парламента, Генеральной прокуратуре, в Министерстве внутренних дел, Оперативно-аналитическом центре, Комитете государственной безопасности (КГБ), Госпогранкомитете, Департаменте финансовых расследований Комитета государственного контроля, Государственном таможенном комитете. Мы получили ответы из Департамента финансовых расследований Комитета государственного контроля и Государственного таможенного комитета.

Мы также отправили обращения аналогичного содержания и просьбы предоставить информацию мобильным провайдерам Life, МТС (Беларусь) и Velcom, а также в их материнские компании Telekom Austria Group, América Móvil, Teliasonera и Turkcell. Мы также написали в «Белтелеком» и в социальную сеть «ВКонтакте». Мы получили ответы из Teliasonera и Telekom Austria Group, и провели телефонные переговоры с представителями Telekom Austria Group.

Ответы, которые мы получили, отражены в соответствующих разделах доклада.

3. ОБЩИЕ СВЕДЕНИЯ

3.1 ОГРАНИЧИТЕЛЬНАЯ ЗАКОНОДАТЕЛЬНАЯ БАЗА В ОТНОШЕНИИ ГРАЖДАНСКОГО ОБЩЕСТВА

В докладе 2013 года «*Что не разрешено, то запрещено: Подавление гражданского общества в Беларуси*» Amnesty International документально засвидетельствовала, что гражданское общество в Беларуси обычно действует в условиях ограничительной правовой среды, в рамках которой нарушаются многие находящиеся под международной защитой права человека.[2] Активисты постоянно сталкиваются с арестами, задержаниями или тюремными заключениями просто за осуществление своих прав.

Неправительственные организации (НКО) в Беларуси сталкиваются с многочисленными бюрократическими требованиями, которые власти зачастую используют для того, чтобы отказать им в регистрации, или закрыть их за несоблюдение этих требований. Например, белорусские власти использовали эти требования, чтобы отказать в регистрации НКО на основании незначительных ошибок в документации, которые легко могли быть устранены.[3] Уголовный кодекс запрещает деятельность незарегистрированных организаций, в том числе политических партий, религиозных групп и НКО.[4]

СМИ жёстко контролируются. Журналистам, работающим с иностранными медиа-организациями, требуется получать правительственную аккредитацию, в которой часто отказывают или задерживают её, а журналистов-фрилансеров, сотрудничающих с иностранными СМИ, штрафуют.[5]

Проведение любых общественных демонстраций или других протестов требует получения разрешения от местных властей, которые редко выдают его. Участие в мирных, но несанкционированных демонстрациях может привести к штрафам или административному аресту.[6]

Другие законы общего применения также усложняют работу активистов. «Оскорбление» или «клевета» на президента или другие органы власти являются уголовными преступлениями.[7] Действительно, клевета и оскорбление как правило наказываются тюремным заключением, в нарушение международных стандартов.[8]

3.2 ИНТЕРНЕТ-СМИ И ПРАВА ЧЕЛОВЕКА В ИНТЕРНЕТЕ

Даже если не касаться вопроса о слежке, условия для реализации прав человека в интернете в Беларуси крайне ограниченны.[9]

Новый закон «О средствах массовой информации», принятый в декабре 2014 года, предоставляет Министерству информации полномочия блокировать доступ к веб-сайтам, не дожидаясь судебного решения. Законом также предусматривается ответственность для владельцев веб-сайтов за незаконный

[2] Amnesty International, «Что не разрешено - то запрещено: Подавление гражданского общества в Беларуси», EUR 49/002/2103, апрель 2013.
[3] Amnesty International, «Что не разрешено - то запрещено: Подавление гражданского общества в Беларуси», EUR 49/002/2103, апрель 2013.
[4] Доклад Amnesty International 2015/2016, Беларусь, https://www.amnesty.org/en/latest/research/2016/02/annual-report-201516/
[5] Доклад Amnesty International 2015/2016, Беларусь, https://www.amnesty.org/en/latest/research/2016/02/annual-report-201516/; см. также, Белорусская ассоциация журналистов, Штрафы журналистам за нарушение статьи 22.9 Административного кодекса (таблица) (обновлено), https://baj.by/en/analytics/fines-journalists-violating-article-229-administrative-code-chart-updated
[6] Amnesty International, «Что не разрешено - то запрещено: подавление гражданского общества в Беларуси», EUR 49/002/2103, апрель 2013.
[7] Уголовный кодекс, статьи 367 - 369.
[8] Уголовный кодекс, статьи 188-9.
[9] См. Индекс цензуры, Беларусь: Закручивание гаек (2013), https://www.indexoncensorship.org/2013/03/belarus-pulling-the-plug/

контент, размещённый пользователями. В результате этого некоторые сайты закрыли разделы, где пользователи оставляли свои комментарии, или перенесли их на отдельные сайты.[10]

В течение 2015 года несколько популярных сайтов правозащитных групп или независимых новостных сайтов – в их числе «Хартия 97», «Белорусский партизан» и «Вясна» – были временно заблокированы. Список заблокированных сайтов не обнародован.[11]

Принятое в феврале 2015 года решение Оперативно-аналитического центра при президенте (ОАЦ) расширить полномочия Министерства информации по блокировке сайтов, создаёт законодательную базу для того, чтобы блокировать не только запрещённый контент, но и средства обеспечения анонимности, которые могли бы использоваться для доступа к заблокированному контенту, такие как «Tor», прокси-серверы или сети VPN.[12] И хотя пока эти инструменты, по всей видимости, ещё не заблокированы, правительство, похоже, разместило тендер на обслуживание инструмента, позволяющего отслеживать и идентифицировать подобные средства обеспечения анонимности.[13]

[10] Интервью с интернет-экспертами, Вильнюс, август 2015; интервью с владельцем сайта, Минск, декабрь 2015.
[11] http://www.belgie.by/ru/lists_access
[12] См. раздел «Шифрование и обеспечение анонимности онлайн», ниже.
[13] https://baj.by/en/content/belarus-authorities-switch-automatic-blocking-anonymizers

4. СКОВЫВАЮЩИЙ ЭФФЕКТ: ЖИЗНЬ В УСЛОВИЯХ СЛЕЖКИ

Опасения по поводу слежки[14] широко распространены среди активистов гражданского общества в Беларуси, и даже среди тех, кто живёт в изгнании. Недостаточные меры по регулированию и надзору, отсутствие возможности оспорить слежку означают, что у активистов просто нет другого выбора, кроме как предположить, что за ними постоянно следят. Поскольку за многие законные виды деятельности – в том числе журналистскую работу без правительственной аккредитации, работу в незарегистрированной организации или за участие в мирной несанкционированной демонстрации – в Беларуси предусмотрена административная или даже уголовная ответственность, активисты зачастую опасаются, что слежка за их повседневной деятельностью может подвергнуть их опасности судебного преследования. Это опасение усиливается в свете памятных репрессий, последовавших за выборами 2010 года, когда частные коммуникации и данные о местонахождении – полученные в результате слежки или как-либо ещё – играли очень заметную роль в ряде политически мотивированных судебных процессов над оппозиционными политиками и другими активистами.

«ДАЖЕ САМА ВОЗМОЖНОСТЬ ТОГО, ЧТО КОММУНИКАЦИИ МОГУТ БЫТЬ ПЕРЕХВАЧЕНЫ, ЯВЛЯЕТСЯ ВМЕШАТЕЛЬСТВОМ В ЧАСТНУЮ ЖИЗНЬ, ЧТО ОКАЗЫВАЕТ ПОТЕНЦИАЛЬНЫЙ СКОВЫВАЮЩИЙ ЭФФЕКТ НА ПРАВА ЧЕЛОВЕКА, В ТОМ ЧИСЛЕ НА ПРАВО НА СВОБОДУ ВЫРАЖЕНИЯ МНЕНИЙ И ПРАВО НА СВОБОДУ ОБЪЕДИНЕНИЙ».

ВЕРХОВНЫЙ КОМИССАР ПО ПРАВАМ ЧЕЛОВЕКА ОРГАНИЗАЦИИ ОБЪЕДИНЁННЫХ НАЦИЙ[15]

Сковывающий эффект, вызванный страхом перед слежкой, проявляется по-разному. Обычно активисты опасались обсуждать какие-либо серьёзные вопросы по телефону или по электронной почте, даже находясь в своих офисах или у себя дома. Поэтому для обсуждения серьёзных вопросов часто возникает необходимость в личной встрече. Однако страх перед слежкой осложняет также и личные встречи; активисты зачастую опасаются, что их мобильные телефоны могут использоваться для отслеживания их местоположения или прослушивания их разговоров, или что за ними может вестись физическая слежка или запись с помощью прослушивающих устройств. Кроме того, активисты опасаются, что власти могут получить доступ к их имейлам или другим цифровым коммуникациям в результате взлома или конфискации электронных устройств. Эти факторы делают использование шифрования и других средств сохранения

[14] Термин «слежка» или «тайное наблюдение» в этом документе относится ко всем видам наблюдения или мониторинга за телефонами, мобильными телефонами, интернетом, или другими данными о коммуникациях, как в режиме реального времени, так и путём получения доступа к сохранённым данным, в том числе содержанию коммуникаций, данным о местонахождении или другим метаданным, связанным с коммуникациями. Он также включает в себя аудио- или видеонаблюдение за людьми или помещениями.

[15] Верховный комиссар по правам человека ООН, «Право на неприкосновенность частной жизни в цифровую эпоху», A/HRC/27/37, 30 июня 2014 (здесь и далее ВКПЧ ООН «Неприкосновенность частной жизни в цифровую эпоху»), пар. 20.

конфиденциальности принципиально важным для активистов, и тем не менее слежка и сковывающий эффект, который она порождает, затрудняют практически любой вид ежедневной деятельности активистов.

4.1 ПОВСЕМЕСТНЫЕ ПОДОЗРЕНИЯ В ИСПОЛЬЗОВАНИИ СЛЕЖКИ

> «БОЛЬШИНСТВО ЛЮДЕЙ БОЯТСЯ ОТКРЫТО РАЗГОВАРИВАТЬ ПО ТЕЛЕФОНУ. ЭТО УЖЕ КАК ЧАСТЬ ВАШЕГО ОБРАЗА МЫСЛЕЙ. ВЫ С САМОГО НАЧАЛА ДОПУСКАЕТЕ, ЧТО ЖИВЁТЕ В СТРАХЕ, ЧТО ВСЁ ПЛОХО, ЧТО ВЫ НЕ МОЖЕТЕ ЭТО КОНТРОЛИРОВАТЬ ИЛИ ИЗМЕНИТЬ».
>
> **НЕЗАВИСИМЫЙ ЖУРНАЛИСТ, МИНСК, ДЕКАБРЬ 2015**

Активисты, журналисты, члены оппозиционных партий и другие люди, которые разговаривали с Amnesty International – как в Беларуси, так и за её пределами – практически единодушно выражали подозрение по поводу того, что за их коммуникациями велось наблюдение.[16] Один из журналистов заметил, что опасение по поводу тайной слежки отрицательно сказывается на жизни и работе активистов и «вызывает ощущение паранойи», однако добавил, что такое ощущение «в данной ситуации вполне оправданно».[17] Ещё один независимый журналист заявил, что из-за его профессии «конечно, они нас прослушивают».[18] Активист, заявивший, что он уверен в том, что власти прослушивали телефонные разговоры активистов, упомянул о том, что мобильные телефоны среди активистов часто в шутку называли «карманным милиционером».[19] Другой активист заявил Amnesty International, что «в принципе, если я разговариваю в помещении, или по телефону, или пишу имейлы, я допускаю, что всё это попадает в КГБ[20]. Поэтому я не обращаю на это внимания и свободно разговариваю, но говорю лишь то, что сказал бы, если бы сотрудник КГБ сидел рядом со мной».[21]

[16] Интервью в Минске, декабрь 2015 ; Интервью в Вильнюсе, август 2015, Интервью в Варшаве, август 2015.
[17] Интервью с независимым журналистом, Минск, декабрь 2015.
[18] Интервью с независимым журналистом, Минск, декабрь 2015.
[19] Интервью с правозащитниками, Минск, декабрь 2015.
[20] Комитет государственной безопасности
[21] Интервью с молодёжным активистом, Минск, декабрь 2015.

ИСПОЛЬЗОВАНИЕ СЛЕЖКИ В ХОДЕ РЕПРЕССИЙ, ПОСЛЕДОВАВШИХ ЗА ВЫБОРАМИ 2010 ГОДА

В ходе репрессий, последовавших за весьма спорными выборами 2010 года, множество людей было арестовано за реализацию своих прав, в том числе за участие в мирных протестах против результатов выборов. Использование слежки за мобильными телефонами и интернет-данными для того, чтобы установить личности протестующих, преследовать оппозиционных политических лидеров и других активистов, стало отличительной чертой этих репрессий. И хотя в последующие годы Беларусь не сталкивалась с репрессиями такого же масштаба, эти события – в том числе ряд получивших широкое освещение в прессе судебных процессов – многие люди, разговаривавшие с Amnesty International, назвали главной причиной своей уверенности в том, что им может угрожать слежка со стороны государства.

После протестов, последовавших за выборами, многочисленные СМИ сообщали о том, что власти использовали данные о мобильных телефонах, чтобы определить, кто присутствовал в местах проведения протестов, и вызывать тех, кого вычислили, на допросы.[22]

Кроме того, некоторые кандидаты от оппозиции выражали опасения по поводу слежки, которая велась в преддверии выборов, а в отношении ряда оппозиционных кандидатов, которые подверглись судебному преследованию после выборов, на суде в качестве доказательств были использованы данные об их личных коммуникациях.[23] Бывший кандидат в президенты от оппозиции Николай Статкевич был заключён в тюрьму за участие в мирных протестах против результатов выборов 2010 года; Amnesty International признала его узником совести. Он вышел на свободу в августе 2015 года. Он рассказал Amnesty International, что в ходе допросов следователи показывали ему расшифровки его разговоров по телефону и по Скайпу, а также расшифровки разговоров его друзей и единомышленников. Он считает, что эти записи были получены без законных оснований.[24]

Андрей Санников, ещё один бывший кандидат в президенты, говорит, что в ходе допросов в рамках уголовного дела, последовавшего за выборами, ему зачитывали выдержки из частных телефонных разговоров. Он говорит, что хотя власти для обоснования этой слежки ссылались на ведущееся в его отношении уголовное расследование, он выяснил, что на самом деле слежка началась за много месяцев до начала расследования. Тогда он выразил протест по поводу того, что ранее осуществлявшаяся за ним слежка велась без каких-либо законных оснований.[25] Санников был заключён в тюрьму за своё участие в протестах, последовавших за выборами; Amnesty International признала его узником совести.[26] До этого, в сентябре 2010 года, в ходе предвыборной кампании его также допрашивали в связи со смертью его друга и пресс-секретаря кампании, Олега Бебенина. В ходе этих допросов ему рассказали о том, каким образом отслеживалось его местонахождение: «Они задавали мне конкретные вопросы о том, что мы обсуждали с Олегом в определённое время. А когда я спросил «Откуда вы это знаете?», – мне показали, каким образом отслеживалось наше местонахождение, и объяснили, как можно отслеживать наши телефоны […] очень точно, в пределах от одного до трёх метров. И они доказали мне это, потому что я точно помню, когда мы встречались, и точно помню, где мы встречались, и мне доказали, что они отслеживали нас; не просто отслеживали: они сказали, что компания, провайдер мобильной связи, может предоставить информацию о точном местонахождении, если этого потребуют прокуратура или милиция […] Это было накануне кампании, так что, конечно, я должен был принять это во внимание».[27]

Алесь Беляцкий, председатель правозащитного центра «Вясна», был арестован в 2011 году по обвинению в уклонении от уплаты налогов. «Вясна» оказывала поддержку жертвам последовавших после выборов репрессий. Amnesty сочла выдвинутые против Беляцкого обвинения политически мотивированными и заявила, что он является узником совести и должен выйти на свободу.[28] Он сообщил Amnesty International: «Фрагменты моего разговора по Скайпу с партнёрами из польской НКО

действительно были опубликованы в государственной газете – «Советская Белоруссия» [сейчас она называется «Беларусь сегодня»] – одной из ведущих газет. Таким образом они пытались скомпрометировать меня, будто бы я искал источники финансирования, чтобы свергнуть режим и так далее, но на самом деле я обсуждал поддержку жертв политических репрессий. Разговор состоялся весной 2011 года, а в газете его опубликовали осенью 2011 года, сразу после моего ареста. Я не знаю, как им удалось прочитать его, вероятнее всего, это была моя ошибка. Скорее всего, я забыл выйти из программы, или может быть, они как-то узнали пароль. Это не было приобщено к обвинению, этого не было в материалах дела, однако это было опубликовано в газете, потому что тем самым они пытались создать атмосферу недоверия в отношении правозащитников... В любом случае, мне кажется, что они могли получить доступ к моему аккаунту в Скайпе прямо тогда, когда проходил разговор, весной, в режиме реального времени. Диск был зашифрован. Так что скорее всего, они как-то перехватили разговор. На суде фигурировали показания экспертов о том, что они не могли считать информацию с дисков».[29]

В последние годы не отмечалось повторения столь же суровых репрессий, какие последовали за выборами 2010 года и связанными с ними протестами. Выборы в 2015 году не сопровождались массовыми протестами и арестами, как в 2010 году. Кроме того, в период, предшествовавший выборам 2015 года, на свободу досрочно вышли несколько деятелей оппозиции, заключённые в тюрьму после выборов 2010 года.[30] Тем не менее, выборы 2015 года подверглись критике со стороны наблюдателей из Организации по безопасности и сотрудничеству в Европе (ОБСЕ), заявивших, что «было отмечено, что Беларуси всё ещё предстоит преодолеть значительный путь для выполнения принятых в рамках ОБСЕ обязательств по обеспечению демократических выборов».[31] Помимо этого, после выборов Специальный докладчик ООН по вопросу о положении в области прав человека в Беларуси отметил, что «положение с правами человека в стране по-прежнему остаётся плачевным».[32]

События 2010 и 2011 годов, в том числе широко освещавшееся использование персональных данных для отслеживания местонахождения людей или их судебного преследования, многие из тех, кто говорил с Amnesty, назвали в качестве причины того, что они по-прежнему опасаются слежки за собой. Многие выражали озабоченность по поводу того, что нынешняя, сравнительно свободная в отношении прав человека среда, не просуществует долго, и изменения политической ситуации могут вновь привести к такому же подавлению прав человека, какое уже случалось в недавнем прошлом. Как выразился один из активистов: «У нас сейчас своего рода вегетарианские времена. Мы не знаем, как долго они продлятся».[33]

В деле *Роман Захаров против России*, Европейский суд по правам человека отметил, что тайная слежка может нанести ущерб правам даже тех людей, которые не являлись её объектами. ЕСПЧ указал, что там, где система тайной слежки может отразиться на любом человеке и там, где не имеется соответствующих средств правовой защиты для того, чтобы оспорить предполагаемое тайное наблюдение:

---

[22] См.: Белорусских оппозиционеров ловят в мобильной сети, 5 января 2011, https://www.rt.com/politics/minsk-mobile-phones-protesters/; Как Teliasonera сотрудничает с диктаторами, Uppdrag Granskning: Чёрные ящики, миссия: расследование, https://vimeo.com/41248885; Human Rights Watch, Сломленные надежды: репрессии после выборов в Беларуси, сноска 31 (март 2011), https://www.hrw.org/report/2011/03/14/shattering-hopes/post-election-crackdown-belarus; «Хартия 97», «О событиях 19 декабря КГБ допрашивает несовершеннолетних», 17 января, 2011, https://charter97.org/ru/news/2011/1/17/35277/ and Warsaw 7.

[23] Тайны президентской кампании. Как шпионят за кандидатами: http://naviny.by/rubrics/elections/2010/12/19/ic_articles_623_171727/?_sm_au_=iVVLpMFqWVFfsQ58

[24] Интервью с Николаем Статкевичем, Минск, декабрь 2015.

[25] Андрей Санников: Лукашенко должен уйти в отставку уже только за прослушку моих телефонов, https://charter97.org/be/news/2011/7/5/40243/?_sm_au_=iVVk6775DJ0jQ5j7

[26] Беларусь: подробнее: Узник совести вышел на свободу: Андрей Санников, https://www.amnesty.org/en/documents/eur49/004/2012/en/

[27] Интервью с Андреем Санниковым, Варшава, август 2015.

[28] Amnesty International, Беларусь: Алесь Беляцкий вышел на свободу по амнистии, https://www.amnesty.org/en/documents/eur49/008/2014/en/

[29] Интервью с Алесем Беляцким, Минск, декабрь 2015; см. также: http://www.sb.by/peredovitsa/article/za-kulisami-odnogo-zagovora.html

[30] Amnesty International США, Беларусь: Политзаключённые вышли на свободу, однако власти должны сделать больше для обеспечения прав человека, http://blog.amnestyusa.org/europe/belarus-political-prisoners-released-but-authorities-need-to-do-more-for-human-rights/

[31] Президентские выборы в Республике Беларусь, 11 октября 2015, ОБСЕ/БДИПЧ Итоговый доклад наблюдательной миссии на выборах, http://www.osce.org/odihr/elections/belarus/218981?download=true

[32] http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17027&LangID=E#sthash.o5jDbz0w.dpuf

[33] Интервью с независимым журналистом, Минск, декабрь 2015.

«НЕЛЬЗЯ ГОВОРИТЬ О ТОМ, ЧТО ШИРОКОМАСШТАБНЫЕ ПОДОЗРЕНИЯ И ОЗАБОЧЕННОСТЬ В ОБЩЕСТВЕ ПО ПОВОДУ ЗЛОУПОТРЕБЛЕНИЙ ПОЛНОМОЧИЯМИ ПО ОСУЩЕСТВЛЕНИЮ СЕКРЕТНОЙ СЛЕЖКИ ЯВЛЯЮТСЯ НЕОПРАВДАННЫМИ [...]. В ПОДОБНЫХ ОБСТОЯТЕЛЬСТВАХ ДАННАЯ УГРОЗА САМА ПО СЕБЕ МОЖЕТ ОГРАНИЧИТЬ СВОБОДНЫЙ ОБМЕН ИНФОРМАЦИЕЙ ЧЕРЕЗ ПОЧТОВЫЕ И ТЕЛЕКОММУНИКАЦИОННЫЕ СЕРВИСЫ, ТЕМ САМЫМ ПРЕДСТАВЛЯЯ ДЛЯ ВСЕХ ПОЛЬЗОВАТЕЛЕЙ ИЛИ ПОТЕНЦИАЛЬНЫХ ПОЛЬЗОВАТЕЛЕЙ ПРЯМОЕ ВМЕШАТЕЛЬСТВО В ИХ ПРАВО [НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ И СЕМЕЙНОЙ ЖИЗНИ]».

РОМАН ЗАХАРОВ ПРОТИВ РОССИИ, ЕВРОПЕЙСКИЙ СУД ПО ПРАВАМ ЧЕЛОВЕКА, ПАРАГРАФ 171.

Некоторые активисты подчёркивали, что сохраняющаяся неопределённость в отношении того, велась ли за ними тайная слежка, крайне негативно сказалась на их психологическом состоянии и на их образе жизни. Многие активисты говорили Amnesty International, что сохранение конфиденциальности в отношении деликатных вопросов – в частности, связанных с их финансированием или общественной деятельностью – было их основной заботой. Один из активистов сказал, что подобные меры безопасности затрудняют организацию и привлечение новой аудитории. Он сказал: «Я совершенно уверен, что КГБ прослушивает нас», но что тем не менее «мы стараемся не бояться этого слишком сильно».[34]

«ТАКОЙ ОБРАЗ ЖИЗНИ УЖЕ СТАЛ ПРИВЫЧНЫМ. [ОПАСЕНИЕ ПО ПОВОДУ СЛЕЖКИ] ОБЯЗЫВАЕТ ВАС К ВЫСОКОНРАВСТВЕННОЙ ЖИЗНИ. ВЫ ПОНИМАЕТЕ, ЧТО НЕ МОЖЕТЕ ПОЗВОЛИТЬ СЕБЕ ПИТЬ СЛИШКОМ МНОГО И ТАК ДАЛЕЕ. ВЫ ОСОЗНАЁТЕ, ЧТО СЛЕЖКА МОЖЕТ ВЕСТИСЬ ЗА ВАМИ В ЛЮБОЙ МОМЕНТ. Я НАСТОРОЖЕННО

[34] Интервью с молодёжным активистом, Минск, декабрь 2015.

ОТНОШУСЬ К ЗНАКОМСТВУ С НОВЫМИ ЛЮДЬМИ. Я НЕ ОБЩАЮСЬ С ТЕМИ, КТО КО МНЕ ОБРАЩАЕТСЯ. Я ОБЩАЮСЬ ТОЛЬКО С ТЕМИ, У КОГО ЕСТЬ РЕКОМЕНДАЦИИ ОТ ЛЮДЕЙ, КОТОРЫХ Я ДЕЙСТВИТЕЛЬНО ХОРОШО ЗНАЮ».

НЕЗАВИСИМЫЙ ЖУРНАЛИСТ, ВАРШАВА, АВГУСТ 2015

Другой активист подчеркнул, что было трудно понять, как вести себя осторожно, если за тобой следят, так как трудно понять, какая информация может быть использована против тебя, и каким образом это может быть сделано: «Все люди чувствуют, что им есть что скрывать. Даже если здесь и нечего скрывать, это всё равно может быть использовано против вас… Мне нечего скрывать, но иногда вы не знаете, что именно вам нужно скрывать».[35] Некоторые люди подчёркивали, что это чувство неуверенности усугублялось отчасти ещё и подозрением, что личная информация, полученная в результате тайной слежки, может быть использована не для уголовного преследования, но для того, чтобы компрометировать людей, используя информацию об их личной жизни.[36]

В отсутствие доступной общественности информации об истинном характере тайного наблюдения, слухи, анекдоты, происшествия, которые могут на самом деле не иметь отношения к тайному наблюдению, иногда воспринимаются активистами как показатель того, что слежка ведётся, что увеличивает страх. Как заметил по поводу тайного наблюдения один белорусский интернет-эксперт, «людям уже достаточно чувствовать, что она существует».[37] Даже те люди, у которых были доказательства того, что власти использовали против них – или опубликовали - их собственные цифровые коммуникации (например, личные чаты в Скайпе), не могли бы с уверенностью сказать, была ли эта информация перехвачена в результате слежки или получена каким-то другим способом.[38] Некоторые люди упоминали случаи, когда их аккаунты в социальных сетях становились доступны онлайн, в то время как сами они находились под стражей; подобные случаи увеличивали у них и их друзей опасения по поводу слежки, несмотря на отсутствие доказательств того, как это могло произойти.[39] Другой оппозиционный активист заметил, что люди склонны рассматривать любое необычное поведение электронных устройств как доказательство ведущейся слежки, даже если на самом деле оно совершенно с этим не связано. Например, он заметил, что если батарея мобильного телефона садится быстрее, чем обычно, это зачастую воспринимается как доказательство ведущейся слежки.[40] Другие также отмечали необъяснимые случаи, которые усиливали опасения по поводу слежки. Один из активистов заявил, что видел расшифровки частных, как он считал, встреч, на которых он присутствовал, размещённые на вебсайтах, считающихся проправительственными. Это убедило его, что за размещением этих материалов в интернете стояли власти.[41]

4.2 КАК ОБЩАТЬСЯ

Если жить в постоянном страхе перед слежкой, то многие простые повседневные действия создают серьёзные трудности, особенно для активистов. Например, большинство людей, говоривших с Amnesty

[35] Интервью активистом по защите окружающей среды, Минск, декабрь 2015.
[36] Интервью с правозащитником, Минск, декабрь 2015; Интервью с оппозиционным политическим активистом, Вильнюс, август 2015; Интервью с оппозиционным политическим активистом, Минск, декабрь 2015.
[37] Интервью с интернет-экспертом, Минск, декабрь 2015.
[38] Интервью с молодёжным активистом и правозащитником, Минск, декабрь 2015.
[39] Интервью с независимым журналистом, Минск, декабрь 2015; Интервью с молодёжным активистом, Минск, декабрь 2015.
[40] Интервью с оппозиционным политическим активистом, Варшава, август 2015.
[41] Интервью с молодёжным активистом, Минск, декабрь 2015.

International, подчёркивали, что не доверяют большинству средств коммуникации, и предпочитают встречаться лицом к лицу, чтобы обсуждать свою работу, в том числе особо важные вопросы.[42]

Разные люди имеют различные мнения по поводу того, какие виды информации представляют особую важность, но чаще всего в этой связи упоминалась финансовая информация и сведения об общественной деятельности или протестах.[43] У активистов также имелись собственные методы общения по телефону в случае необходимости. Оппозиционная активистка рассказала о том, что она использовала предварительно оговоренный код для того, чтобы поговорить с коллегами по телефону.[44] У других групп были правила для безопасного общения, которые включали, в частности, такой пункт - никогда не обсуждать места встреч по телефону.[45] Другой активист подчеркнул, что обсуждает по телефону только публичную информацию или разговаривает на общие темы.[46]

Молодёжный активист заметил, что «Мы не обсуждаем важные вопросы по телефону или в интернете. Мы стараемся обсуждать самые важные вещи лично на встречах, где можно общаться лицом к лицу. Сейчас мы используем интернет для организации встреч, но никогда не обсуждаем ничего, что может представлять для нас опасность в этой связи. Мы никогда не обсуждаем конкретные детали наших мероприятий и не называем людей или организации».[47]

> «НАШИ ТЕЛЕФОНЫ…НАШИ ПРОВАЙДЕРЫ, ПРЕДОСТАВЛЯЮЩИЕ МОБИЛЬНУЮ СВЯЗЬ, ВСЕ ОНИ СОТРУДНИЧАЮТ С ПРАВИТЕЛЬСТВОМ[48]…ПОЭТОМУ МЫ ПРЕДПОЧИТАЕМ НЕ ГОВОРИТЬ О ДЕНЬГАХ, ИЛИ МЕСТАХ, ГДЕ МЫ ВСТРЕЧАЕМСЯ, ГДЕ ГОВОРИМ О РАЗНЫХ СЕРЬЁЗНЫХ ВЕЩАХ И ОБО ВСЁ ЭТОМ. У НАС ДАЖЕ ЕСТЬ СПЕЦИАЛЬНЫЕ КОДЫ, С ПОМОЩЬЮ КОТОРЫХ МЫ МОЖЕМ ГОВОРИТЬ О ДЕНЬГАХ».
>
> **АКТИВИСТ, ОТСТАИВАЮЩИЙ ПРАВА ЛГБТИ, УДАЛЁННОЕ ИНТЕРВЬЮ ИЗ ЛОНДОНА, АПРЕЛЬ 2016**

Оппозиционный активист, говоря о трудностях, с которыми он сталкивается при разговорах по телефону - в том числе об использовании вымышленных имён и закодированных названий мест, пожаловался: «это на самом деле раздражает, так как вам приходится жить в этом режиме. Вы знаете, здорово раздражает, когда вы не можете говорить открыто, не можете говорить по телефону, не приняв мер предосторожности».[49]

Один из правозащитников сказал Amnesty International: «Я вообще не пользуюсь стационарными телефонами. Своим личным мобильным телефоном я пользуюсь только для организации встреч. Я уверен, что за моим мобильным телефоном установлена слежка. Я знаю, что у них есть техническая возможность

[42] Интервью в Минске, декабрь 2015 и Вильнюсе, август 2015.
[43] Интервью с активистами в Минске, декабрь 2015, в Вильнюсе, август 2015 и в Лондоне, апрель 2016.
[44] Интервью с оппозиционным политическим активистом, Минск, декабрь 2015.
[45] Интервью с правозащитниками, Минск, декабрь 2015.
[46] Интервью с правозащитниками, Минск, декабрь 2015.
[47] Удалённое интервью с молодёжным активистом, Лондон, март 2016.
[48] «Операторы мобильной связи в Беларуси предоставляют властям прямой, автоматический доступ к данным пользователей». См. раздел: «Что такое «СОРМ»?
[49] Интервью с оппозиционным политическим активистом, Варшава, август 2015.

определить моё местоположение, используя мой мобильный телефон. Вот почему когда мне нужно остаться неузнанным, сохранить инкогнито, я оставляю свой телефон в офисе».[50]

4.3 КАК ВСТРЕЧАТЬСЯ

Наряду с тем, что страх перед слежки, распространённый среди активистов гражданского общества, делает необходимым личные встречи, он также затрудняет и усложняет их. Большинство активистов, с которыми разговаривала Amnesty International, были озабочены тем, что их мобильные телефоны могли использоваться для удалённой записи их встреч, или могли позволить определить их местоположение – и таким образом установить, с кем они встречаются. Кроме того, многие опасались, что в их офисах установлены прослушивающие устройства, из-за чего необходимо находить общественные места и там встречаться для обсуждений с глазу на глаз.

Некоторые активисты отметили, что не берут свои мобильные телефоны на встречи из-за опасений по поводу слежки.[51]

> «НЕКОТОРЫЕ ВИДЫ ДЕЯТЕЛЬНОСТИ – ОБСУЖДЕНИЕ НЕ САМЫХ ОТКРЫТЫХ ТЕМ – МЫ, КОНЕЧНО, ПРОВОДИМ БЕЗ МОБИЛЬНЫХ ТЕЛЕФОНОВ, ПРИ ЭТОМ МЫ СТАРАЕМСЯ, ЧТОБЫ ВСТРЕЧИ ОРГАНИЗОВЫВАЛИ ПОСРЕДНИКИ, ДА, ЭТО ТА ЦЕНА, КОТОРУЮ НАМ ПРИХОДИТСЯ ПЛАТИТЬ».
>
> **ИНТЕРВЬЮ С НЕЗАВИСИМЫМ ЖУРНАЛИСТОМ, МИНСК, ДЕКАБРЬ 2015**

Молодёжный активист из незарегистрированной организации рассказал, как он и его коллеги использовали заброшенные здания для того, чтобы проводить встречи, избегая слежки.[52]

Один из активистов заметил, что такие способы организации встреч порождены ограничениями, которые накладывает это время. По большому счёту, заметил он, ему приходилось организовывать личные встречи просто чтобы люди встретились, вместо того, чтобы использовать более простые способы – например, разговоры по телефону.[53] Другой активист посетовал, что без слежки «многие вещи были бы проще. Довольно трудно, когда для того, чтобы что-то обсудить, нужна личная встреча. В 21-м веке мы всё ещё вынуждены встречаться с глазу на глаз, как в 1990-е годы».[54]

4.4 ВАЖНОСТЬ ШИФРОВАНИЯ

Тайное наблюдение и связанные с ним опасения делают использование шифрования крайне важным для белорусских журналистов, активистов и других жителей страны. Почти каждый, кто разговаривал с Amnesty International, особо выделял важность для своей работы шифрованных коммуникаций или устройств

[50] Удалённое интервью с правозащитником, Лондон, май 2016.
[51] Интервью в Минске, декабрь 2015, в Вильнюсе, август 2015, и удалённое интервью из Лондона, май 2016.
[52] Интервью с молодёжным активистом, Минск, декабрь 2015.
[53] Интервью с оппозиционными политическими активистами, Вильнюс, август 2015.
[54] Интервью с молодёжным активистом, Минск, декабрь 2015.

шифрования.[55] Как заметил один из активистов, такие инструменты «абсолютно необходимы».[56] Один из студенческих активистов сказал Amnesty International: «всё, что связано с работой, всегда шифруется с помощью PGP,[57] и я никогда не обсуждаю что-либо, связанное с работой, по Скайпу».[58]

ШИФРОВАНИЕ И ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ ОНЛАЙН

Шифрование является математическим процессом преобразования сообщений, информации или данных в такую форму, в которой её не может прочитать никто, кроме получателя (и, в зависимости от типа шифрования, провайдера).

Шифрование содержания коммуникаций не обеспечивает конфиденциальности: поскольку инструменты шифрования обеспечивают, чтобы содержание коммуникации могло быть расшифровано только теми, у кого имеется ключ для дешифровки, они не гарантируют анонимность ни получателя, ни отправителя. Определение участников коммуникации возможно и в том случае, когда они используют шифрование, так как метаданные, связанные с коммуникацией, не шифруются. Если кто-то хочет сохранить анонимность, ему нужно использовать средства и методы сохранения конфиденциальности, например, использовать псевдонимы или средства сохранения конфиденциальности, такие как специальный веб-браузер «Tor».[59]

И хотя шифрование и средства сохранения конфиденциальности во многих случаях помогают сохранить конфиденциальность коммуникаций, они не могут гарантировать неприкосновенность частной жизни при любых обстоятельствах, и остаются уязвимыми для взлома, пользовательских ошибок и других факторов.

В эпоху цифровых технологий доступ к использованию шифрования является средством обеспечения права на неприкосновенность частной жизни, права на свободу выражения мнений, права на свободу информации и убеждений, а также затрагивает права на свободу мирных собраний, свободу объединений и другие права человека. Шифрование является особенно важным инструментом для правозащитников, активистов и журналистов, которые всё чаще полагаются на него для того, чтобы обеспечить безопасность – свою и других. Amnesty International считает, что государства должны содействовать использованию шифрования и не должны неоправданно вмешиваться или позволять кому-либо вмешиваться в эту область.[60]

Более подробную информацию об инструментах, которые могут быть использованы для защиты неприкосновенности коммуникаций, вы можете найти на странице «Самостоятельная защита от слежки» ресурса Electronic Frontier Foundation[61] или на странице проекта «Всё о безопасности» ресурса Tactical Technology Collective and Frontline Defenders.[62]

Один из ЛГБТИ-активистов сказал, «Небезопасно использовать любое оборудование «Белтелекома» без применения средств защиты. Поэтому мы с самого начала поняли, что нам нужно использовать VPN-соединение…[63] Финансовые вопросы – это один из главных моментов, в отношении которых у властей имеется механизм оказания давления на нас. Поэтому иногда на эту тему […] нельзя говорить, когда вы не чувствуете себя в безопасности. Вы никогда не будете обсуждать это в кафе. Вы не будете упоминать имён, и так далее. Не все из тех, кто жертвуют нам деньги, достаточно хорошо понимают, насколько опасным это может быть, хотя иногда это не очень удобно для них. Потому что вы на самом деле не можете просто написать письмо и отправить его, чтобы всё было в порядке. Мы просим их использовать защищённые почтовые ящики, PGP-связь и всё это. Так что сейчас мы общаемся с ними именно так, и они понимают, насколько важно это может быть».[64]

---

[55] Интервью в Минске, 2015 и Вильнюсе, август 2015.
[56] Интервью с независимым журналистом, Минск, декабрь 2015.
[57] Система межабонентского шифрования электронной почты, https://ssd.eff.org/en/glossary/pgp
[58] Удалённое интервью со студенческим активистом, Лондон,апрель 2016.
[59] Более подробно о браузере «Tor» см. https://www.torproject.org/about/overview.html.en

[60] См. Amnesty International, «Шифрование в контексте прав человека», https://www.amnesty.org/en/documents/pol40/3682/2016/en/
[61] https://ssd.eff.org/
[62] https://securityinabox.org/
[63] Виртуальная частная сеть
[64] Удалённое интервью с активистом, отстаивающим права ЛГБТИ, Лондон, апрель 2016.

Один из молодёжных активистов пожаловался, что хотя инструменты шифрования и являются необходимыми для активистов, особенно в том, что касается финансовой информации, они могут затруднять работу и даже приводить к работе впустую: «Если вы защищаете всю свою информацию, вы не можете ничего достичь». Он посетовал, что время, которое занимает шифровка и дешифровка информации, невозможность хранить документы в бумажном виде или печатать документы, серьёзно препятствовали работе: «Это непросто. Это совсем не помогает нашей работе. Это делает нашу работу намного менее эффективной. Я ненавижу все эти меры безопасности…[наша организация] исчезнет, станет просто какой-то тайной группой».[65]

4.5 ОПРЕДЕЛЕНИЕ МЕСТОНАХОЖДЕНИЯ ТЕЛЕФОНА/ПРОСЛУШКА

Большая часть тех, с кем провела интервью Amnesty International, лично сталкивались с ситуациями (или что-то слышали о них), заставившими их подозревать, что телефоны прослушивались или отслеживались, хотя эти подозрения обычно невозможно было проверить.

Все жаловались на то, что милиция иногда, казалось, имела информацию о времени и месте проведения некоторых мероприятий ещё до того, как они происходили. Одна журналистка рассказала, что ей часто случалось приехать в город, чтобы встретиться с активистами, с которыми она разговаривала по телефону, только для того, чтобы обнаружить, что милиция уже ожидает её прибытия.[66] Один из активистов отметил, что милиция, казалось, часто была осведомлена о месте проведения тайно организованных протестов заранее.[67] Юрист, занимающаяся защитой прав человека, сообщила, что видела подозрительную машину, на крыше которой была смонтирована антенна, недалеко от места проведения протеста; она подозревает, что таким образом отслеживались мобильные телефоны протестующих.[68]

В других ситуациях информация, которая выяснялась из контактов с властями, или которая следовала из их поведения, могла заставить людей подозревать, что их телефонные разговоры прослушивались. Один из оппозиционных активистов рассказал Amnesty International, как один раз ему позвонил милиционер и предложил встретиться. Активист в то время состоял на учёте в милиции из-за своего участия в протестах, он часто разговаривал с этим милиционером и знал, как его зовут. После этого звонка он позвонил своей жене и рассказал ей о звонке из милиции, назвав звонившего по прозвищу, которым они называли его между собой. Через два часа милиция задержала его на улице. Он сказал, что подозревает, что милиция знала о его местонахождении, отслеживая его телефон. Когда его привезли в отделение, милиционер, который звонил ему, спросил, почему он назвал его по прозвищу. Активист сказал, что он воспринял это как попытку продемонстрировать, что милиция может прослушивать его разговоры.[69]

Тот же активист рассказал о другом случае, который произошёл в 2012 году; тогда, как он считает, его местонахождение было установлено милицией в результате прослушивания его телефонных разговоров: «Однажды я говорил на улице с одним человеком. Мы, насколько я помню, договорились встретиться в 14:10 на вокзале. Я пришёл в 14:00, и в 14:05 я увидел двух милиционеров в штатском, которые явно кого-то поджидали на площади перед вокзалом. Я тогда был довольно неопытным. Поэтому я подумал (ясно помню эту мысль): «Не могут же они ждать меня». Конечно, нет. Некоторое время они ещё подождали, расхаживая туда-сюда минуты три, а потом подошли ко мне и надели на меня наручники. Вот так. И как обычно, меня доставили в здание, расположенное неподалёку. Это было Управление внутренних дел Московского района. Я часто там бываю».[70]

Ещё один активист рассказал похожую историю о том, как милиция арестовала его; он уверен, что милиция узнала о его местонахождении в результате прослушивания его телефона: «Например, был один случай в 2013 году. Это было уже не в первый раз. Я был в Минске, и у меня были назначены несколько встреч. Я шёл на встречу, и ко мне в метро подошли двое милиционеров. Они показали мне свои удостоверения. Это было уже не в первый раз, и я знал, что должно произойти дальше. Поэтому я начал кричать и звать на помощь. После этого другие милиционеры, дежурившие на станции метро, подошли к нам (эти были в форме). Первые двое показали им свои документы. Потом они посадили меня в микроавтобус, и привезли в отделение милиции. Там у нас был разговор с этими двумя парнями. Они были из какого-то спецподразделения, я даже думал, что из ОМОНа, особого отряда милиции. Я не знаю точно, но думаю, что они были не из КГБ. Я говорил с ними по-русски, и они смеялись надо мной и сказали: «Не используй

[65] Интервью с молодёжным активистом, Минск, декабрь 2015.
[66] Интервью с независимым журналистом, Минск, декабрь 2015.
[67] Интервью с интернет-экспертом, Вильнюс, август 2015.
[68] Интервью с правозащитником, Минск, декабрь 2015.
[69] Интервью с молодёжным активистом, Минск, декабрь 2015.
[70] Интервью с молодёжным активистом, Минск, декабрь 2015.

русский язык, когда говоришь по телефону». Я имею в виду, что они дали понять, что прослушивали мои разговоры. Я думаю, они имели в виду разговоры, которые происходили в тот день, они прослушивали их в режиме реального времени. И они даже не были из КГБ, а просто из одного из спецподразделений. Они знали, что у меня встреча, они ждали меня на том месте, где она была назначена».[71]

Одна из правозащитниц рассказала, как сотрудник КГБ, с которым она говорила по телефону, заявил, что знает, где она находится. Она сказала: «Когда меня вызвали на встречу в КГБ, их сотрудник позвонил и сказал «мы вас довезём». Я ответила: «Откуда вы знаете, где я?» Он сказал, что я была на работе, и они заберут меня оттуда. Власти контролировали мои передвижения».[72]

4.6 ПРОСЛУШИВАНИЕ С ПОМОЩЬЮ «ЖУЧКОВ»/ФИЗИЧЕСКАЯ СЛЕЖКА

Физическая слежка, как и установка прослушивающих устройств, «жучков», в офисах и домах, по-прежнему вызывают опасения у многих представителей гражданского общества в Беларуси, затрудняя работу активистов и вынуждая их быть сдержанными при обсуждении важных вопросов в своих собственных офисах.

Одна из правозащитниц заявила, что они не могут быть уверены в том, что в их офисе нет «жучка». Она вспомнила инцидент, произошедший, когда они работали в предыдущем офисе:

«В один из дней мы обнаружили, что [наши соседи снизу] переезжают, и я спросила, почему. Они ответили, что работать здесь стало невозможно, потому что агенты спецслужб раз за разом приходили к ним, чтобы выпроводить их из офиса (вместе с их клиентами) для того, чтобы прослушивать, что происходит в нашем офисе. Это было настолько губительно для их бизнеса, что они вынуждены были переехать.

Любые виды проверок на наличие прослушивающих устройств нельзя считать по-настоящему эффективными, поскольку они показывают только то, что происходит в данный конкретный момент. Это может вызвать ложное чувство безопасности. Теперь у нас создалось такое ощущение, что офис могут прослушивать в любой момент, и это не место для серьёзных разговоров».[73]

Представители оппозиции также выражали уверенность в том, что их офисы, скорее всего, прослушивают. При этом они также заявили, что бесполезно пытаться искать «жучки» в офисе, так как даже если их найти и удалить – это лишь создаст ложное чувство безопасности, раз они могут быть снова установлены в любом месте.[74]

Опасение по поводу того, что их офисы или дома могут прослушиваться, заставляет активистов с подозрением относиться к необъяснимым или необычным происшествиям, которые могут быть связаны со слежкой. Упоминавшаяся выше правозащитница рассказала, как она в прошлом году приехала в сервис на своей машине из-за отказа сигнализации, и мастер обнаружил непонятное устройство, которое, по всей видимости, было микрофоном и не являлось частью противоугонной сигнализации. Она опасалась, что это было прослушивающее устройство, однако не было никакой возможности это проверить.[75]

В связи с отсутствием действительных возможностей получения правовой защиты от тайного наблюдения, активистам остаётся только догадываться о причинах событий, которые, как представляется, связаны со слежкой. Одна активистка рассказала, что её вызвали для разговора в КГБ, и в ходе беседы сотрудник КГБ задавал конкретные вопросы, показывающие, что ему было известно содержание разговоров, которые она недавно вела с международным спонсором. Информация, известная сотруднику КГБ, обсуждалась только на частной встрече со спонсором в Вильнюсе, в машине с другими активистами, и на встрече в её офисе с членами её организации. Активисты предполагали, что информация могла быть получена с помощью прослушивающего устройства в её офисе, или от осведомителей в её организации, однако не было никакого способа проверить, так ли это было на самом деле.[76]

Многие люди выражали опасения, что за ними велась физическая слежка или что за их организациями наблюдали правительственные осведомители, но редко были способны предоставить конкретную информацию на этот счёт.

Один из журналистов, работающий на неаккредитованное информационное агентство, и в связи с этим вынужденный работать в неофициальных офисах, которые находятся в квартирах, рассказал такую

[71] Интервью с оппозиционным политическим активистом, Варшава, август 2015.
[72] Интервью правозащитником, Минск, декабрь 2015.
[73] Интервью с правозащитником, Минск, декабрь 2015.
[74] Интервью с оппозиционным политическим активистом, Минск, декабрь 2015.
[75] Интервью с правозащитником, Минск, декабрь 2015.
[76] Интервью с активистом по защите окружающей среды, Минск, декабрь 2015.

историю: «Мы однажды [в 2008 году] приняли на работу человека, который был специалистом по поиску скрытых устройств, и он обнаружил «жучок» в одной из наших квартир. И на следующий день к нему домой пришли из КГБ, и они не сказали ему «зачем ты нашёл этот «жучок» для них», они сказали ему «кое-кто расписался за этот «жучок», пожалуйста, отдай его нам. Мы финансово ответственны за это устройство, так что ты должен нам его вернуть». И после этого случая мы перестали искать «жучки» в наших квартирах, но я практически на 100% уверен, что они всё ещё там».[77]

Активисты также опасаются за свои собственные дома. Андрей Санников, бывший кандидат в президенты от оппозиции, который был заключён в тюрьму после протестов, последовавших за выборами 2010 года, и которого Amnesty International признала узником совести,[78] рассказал, что он узнал, что в связи с его судебным преследованием в его квартире было установлено прослушивающее устройство, и все разговоры записывались. Он сказал, что он уверен, что квартира, в которой по-прежнему живёт его семья, всё ещё прослушивается.[79]

Ещё один активист, которого множество раз арестовывали за протестную деятельность, заявил, что больше не верит в неприкосновенность своей квартиры. Он рассказал, что когда он и его жена вернулись со свадьбы и обнаружили, что компьютер в их квартире был передвинут. И он, и его жена сначала решили, что кто-то из них передвинул компьютер, но когда выяснилось, что они оба этого не делали, они начали очень нервничать по поводу того, что кто-то побывал в их квартире и что с компьютером что-то делали.[80]

Прослушивающее устройство, обнаруженное в кафе в ходе встречи оппозиционных политиков.

Один из редких случаев, когда было получено вещественное доказательство, свидетельствующее о возможной слежке, произошёл в октябре 2015 года. На встрече оппозиционных политиков в кафе в центре Минска Анатолию Лебедько показалось подозрительным, что подошедший официант поменял держатель для салфеток на их столе. Осмотрев его, он обнаружил, что держатель для салфеток открывается, и в его основании находится что-то, похожее на прослушивающее устройство. Они не были уверены в том, что именно представляет из себя это устройство, поэтому решили забрать его с собой для изучения. Они опасались, что если немедленно известить прессу или милицию, устройство могут конфисковать. После проведения экспертизы было установлено, что это действительно было прослушивающее устройство, и они подали жалобу в Генеральную прокуратуру, требуя провести расследование этого инцидента [см. ниже].[81]

4.7 ВЗЛОМ

Документально зафиксированные случаи взлома – использования программного обеспечения или иных технологий для наблюдения или получения какого-либо доступа к коммуникациям или другой персональной информации или аккаунтам пользователя – всё ещё сравнительно редки в Беларуси, или по крайней мере о них редко сообщается. Активисты не знают, какие средства или инструменты имеются в распоряжении белорусского правительства для взлома компьютеров или телефонов. В июле 2015 года в результате

[77] Интервью с независимым журналистом, Минск, декабрь 2015.
[78] Amnesty International, Беларусь: подробнее: Узник совести вышел на свободу: Андрей Санников, https://www.amnesty.org/en/documents/eur49/004/2012/en/
[79] Интервью с Андреем Санниковым, Варшава, август 2015.
[80] Интервью с молодёжным активистом, Минск, декабрь 2015.
[81] Интервью с «Объединённой гражданской партией», Минск, декабрь 2015; Статкевич, Лебедько и Некляев в ходе встречи в «Салодкім фальварку» обнаружили «жучок» в держателе для салфеток http://nn.by/?c=ar&i=158217&lang=ru .

утечки о деятельности коммерческого поставщика программного обеспечения для слежения за действиями пользователей Hacking Team, были обнародованы документы, которые, по всей видимости, свидетельствуют о том, что ОАЦ и Министерство внутренних дел проявляли интерес к приобретению у Hacking Team инструментов шпионского ПО, в том числе позволяющих получать доступ к выбранному компьютеру и извлекать нужные данные через USB-диск. Документы не содержат доказательств того, что продажа была завершена.82

Там, где случаи взлома, по всей видимости, действительно имели место, обычно не представляется возможным определить, с помощью каких средств был осуществлён взлом, или кем это было сделано. Зачастую эти случаи допускают различные технические объяснения. Как бы там ни было, следующие примеры показывают, что это может, тем не менее, затрагивать права активистов гражданского общества, когда частные имейлы или аккаунты в социальных сетях оказываются под угрозой.

ЛЕОНИД СУДАЛЕНКО

Многие из тех, кто разговаривал с Amnesty International, упоминали об одном эпизоде, который произошёл с Леонидом Судаленко.[83] В январе 2015 года Судаленко, правозащитник из Гомеля, на юго-востоке Беларуси, обнаружил, что его учётная запись на mail.ru заблокирована:

> «Он [почтовый аккаунт на mail.ru] на самом деле был взломан дважды. В первый раз это произошло 6-го января, но тогда мне удалось восстановить его через службы технической поддержки и использовать дальше. Этот аккаунт был важен для меня: я создал его в 1999 году, когда ещё не было Gmail, это был мой официальный имейл, и за эти годы его узнали многие люди. Поэтому я не хотел удалять его, он был для меня ценным.
>
> Когда его взломали в первый раз, я восстановил его и пользовался им ещё две недели. Но когда 20-го числа его снова взломали, я потерял интерес к его использованию. Также я тогда решил, что нужно прекратить пользоваться аккаунтами, расположенными в России. Эти аккаунты не обеспечивают конфиденциальность. Их даже не надо взламывать: русская секретная служба могла легко передать мои пароли белорусской секретной службе».[84]

Ему удалось получить от Mail.ru документы, подтверждающие его усилия по восстановлению своей учётной записи электронной почты.[85] Спустя несколько месяцев, в апреле, в его офис, который он использовал совместно со многими другими организациями гражданского общества, пришла милиция, которая изъяла восемь компьютеров (четыре забрали из офиса, и ещё четыре из дома, часть из них принадлежали его жене и детям) в связи с уголовным расследованием:

> «В тот день я был в Стокгольме. Шведские правозащитники пригласили меня на ежегодную международную правозащитную конференцию. В то время как я был там, мне позвонила жена и сказала, что у нас дома провели обыск, и что они искали не только порнографические материалы, но также и наркотики. Она сказал это, так как проводившие обыск милиционеры были из управления по наркоконтролю. Конечно, я был напуган. У меня двое сыновей-подростков, 14 и 18 лет. Была вероятность, что их как подростков подозревали в чём-то, связанном с наркотиками. Шведские правозащитники предложили мне ещё на некоторое время остаться в Стокгольме, однако я отказался и поехал в

[82] https://www.occrp.org/en/daily/4161-belarus-wanted-to-use-usb-sticks-to-infect-devices-and-collect-data; https://charter97.org/en/news/2015/7/16/160052/
[83] См., например, World Report 2016: Беларусь, Human Rights Watch, https://www.hrw.org/world-report/2016/country-chapters/belarus
[84] Удалённое интервью с Леонидом Судаленко, Лондон, май 2016.
[85] Удалённое интервью с Леонидом Судаленко, Лондон, май 2016.

Беларусь, чтобы доказать свою невиновность. Вернувшись, я попытался выяснить, что произошло. Сегодня мне ясно, что это была спланированная провокацию с целью оклеветать меня. Я уверен, что если бы это не случилось прямо перед президентскими выборами 2015 года, я сейчас был бы в тюрьме. Статьи, по которым предполагалось обвинить меня, не предусматривают иных мер наказания, кроме тюремного заключения от 2 до 4 лет…

Ситуация была следующая. Порнография была отправлена с моего аккаунта (кстати, они послали её не только в налоговую службу, но и в районное следственное управление). Потом на основании этого факта было возбуждено уголовное дело. Требовалось расследовать этот вопрос. Так как порнография была послана с моего аккаунта, они пришли ко мне в офис и домой, чтобы провести там обыски. Они изъяли офисное оборудование. Я заявил, что это провокация с целью клеветы…

После того, как они изъяли компьютеры, меня допросили в следственном управлении. Затем я показал следователю скриншоты, которые доказывали, что администрация mail.ru и я вели переписку по поводу этого взлома [аккаунта на mail.ru]. Позже, после июня 2015 года, была проведена экспертиза. Эксперт сказал, что порнографические материалы были посланы не с наших компьютеров. Потом они вернули нам компьютеры, и на этом всё кончилось. С тех пор следователи меня не беспокоили.

К тому времени многие национальные и международные организации выступили в мою защиту. Они написали президенту, начальнику КГБ и в Министерство внутренних дел. За меня вступились шведские правозащитники, Front Line Defenders и Amnesty International. Кроме того, более 25 известных белорусских правозащитников написали открытое письмо Министру внутренних дел, заявив, что знают меня как законопослушного гражданина и просят прекратить эту провокацию. Специальный докладчик по вопросу о положении правозащитников также был информирован об этой ситуации. Я думаю, что не получи я такой серьёзной поддержки, решение экспертов могло бы быть другим. Что значит экспертиза в Беларуси? Они всегда получают то, что им надо. Поэтому результаты экспертизы могли быть совершенно другими. И если бы эксперт заявил, что установил, что порнография была отправлена с моего компьютера, мне было бы тяжело доказать в суде свою невиновность».[86]

АЛЕКСАНДР

Александр – член политической оппозиционной группы и ЛГБТИ-активист. В 2015 году его аккаунт в социальных сетях был взломан, что привело к проблемам с работодателем. Он уверен, что за взломом его аккаунта в соцсетях стояли власти, и опасался, что его могут привлечь к ответственности. Несмотря на это, он подал заявление о расследовании взлома, для того чтобы защитить себя от возможного судебного преследования, однако его заявление не было принято, не было проведено даже доследственной проверки:

[86] Удалённое интервью с Леонидом Судаленко, Лондон, май 2016.

«Всё это началось в начале 2015 года. К примеру… меня видели онлайн в интернете в то время как я не мог войти в сеть, потому что был с друзьями, и у меня не было доступа к компьютеру.

Было ещё несколько подобных ситуаций, а один раз тот, кто использовал мой аккаунт – кто бы это ни был – даже поменял пароль. Но мне всегда удавалось вновь получить доступ к своему аккаунту, отправив администрации социальной сети сообщение с телефонного номера, который был связан с аккаунтом…

Когда всё это случилось, я связался с администрацией «ВКонтакте» [чтобы получить доступ к данным о моём логине и отследить подозрительную активность], однако они ответили, что раскроют эту информацию только при наличии официального запроса следственных органов».[87]

Через несколько месяцев, в мае 2015 года, у Александра начались проблемы с менеджером в организации, занимавшейся проблемами ВИЧ/СПИД, в которой он работал. Проблемы были связаны с его членством в оппозиционной партии. Он сказал, что тщательно скрывал своё членство в партии, и что он уверен, что эта информация попала в поле зрения менеджера, потому что ему показали личную переписку в социальной сети «ВКонтакте» – подозрения, которые, по его словам, менеджер подтвердил:

«Когда я говорил со своим руководителем, (пытаясь убедить его не увольнять меня), он сказал, что 29 мая 2015 года с ним встретились сотрудники управления по наркоконтролю и противодействия торговле людьми и передали ему распечатки скриншотов моей переписки «ВКонтакте». Он показал мне эти скриншоты в присутствии свидетелей. Я видел их своими собственными глазами…

Это управление также занимается незарегистрированными организациями[88] (зарегистрированными занимается КГБ). Более того, многие ЛГБТИ-активисты подвергались давлению и преследованию со стороны сотрудников этого управления…

«Куратор» (сотрудник управления) сказал моему начальнику, что власти взломали мой аккаунт «ВКонтакте» и, прочитав мои сообщения, выяснили, что я являюсь членом политической партии и связан с правозащитной группой, что означало, что я занимаюсь общественной деятельностью. Этот «куратор» также охарактеризовал меня как «ненадёжного сотрудника» и потребовал, чтобы меня немедленно уволили».[89]

Примерно тогда же, как заявил Александр, он начал получать телефонные звонки с угрозами. И хотя он не мог определить, кто ему звонил, ему угрожали привлечением к ответственности за участие в незарегистрированной организации («Молодые социал-демократы») по статье 193 Уголовного кодекса, что убедило его, что звонившие действовали с ведома властей. Александр обратился в милицию и потребовал расследовать взлом своих аккаунтов:

[87] Интервью с Александром, Минск, декабрь 2015, и удалённое интервью из Лондона, апрель 2016; Amnesty International письменно обратилась к «ВКонтакте» за разъяснениями, однако ответа не получила.
[88] Статья 193.1 Уголовного кодекса запрещает деятельность незарегистрированных организаций (политических партий, религиозных групп, а также НКО), Доклад Amnesty International 2015/2016, https://www.amnesty.org/en/latest/research/2016/02/annual-report-201516/
[89] Интервью с Александром, Минск, декабрь 2015, и удалённо из Лондона, апрель 2016.

«У меня не было надежды [что расследование даст результаты]. Даже если бы они провели тщательное расследование, милиция обнаружила бы милицию. Однако я всё же считал, что важно зарегистрировать у них это заявление, потому что было уже несколько похожих случаев в Беларуси: например, был взломан почтовый аккаунт правозащитника [Леонида] Судаленко [см. выше], с его аккаунта были отправлены дискредитирующие его материалы, после чего в его отношении возбудили уголовное дело. Похожая история произошла с одним из моих коллег: от его имени была отправлена порнография, после чего его привлекли к суду. Поэтому мне нужно было зарегистрировать свою жалобу: чтобы я смог, если потребуется, доказать тот факт, что мой аккаунт был взломан.

Мне нужен был этот отказ, чтобы обезопасить себя. Я не знал, чего ожидать от властей. Они могли возбудить против меня уголовное дело точно так же, как это было сделано с Судаленко».[90]

В ответ на своё заявление о проведении расследования, Александр получил из милиции письмо,[91] в котором говорилось, что милиция отправила в соответствующий департамент Министерства внутренних дел Беларуси запрос о проведении расследования преступления в сфере высоких технологий, но не получили ответа. В письме говорилось, что в связи с отсутствием ответа, они не могут определить, кто именно получил доступ к аккаунту Александра, а также достоверно выяснить, действительно ли вред был причинён в результате действий третьей стороны, а не в результате вирусной атаки. В письме говорилось, что в связи с этим милиция отказывается проводить расследование. Таким образом, по всей видимости, милиция не предприняла никаких шагов для расследования поданной Александром жалобы за исключением отправки запроса, ответа на который не последовало. Александр подал апелляцию на отказ поводить расследование, однако письменного ответа так и не получил. Он говорит, что по его настоянию, ему устроили личную встречу со следователями, которые дали понять, что расследования не будет.[92]

ИВАН

Иван [93]- студенческий активист, помогавший организовать несанкционированные, но мирные демонстрации в университетских кампусах. Он объяснил, что оказался под давлением, и в конце концов был исключён из университета отчасти из-за того, что его личные онлайн-коммуникации оказались взломанными:

«Заместитель декана моего факультета показал мне скриншот переписки между владельцем одного из личных аккаунтов и аккаунтом сообщества [группы студенческих активистов «ВКонтакте»], администратором которого я был. Из скриншота было видно, кто из администраторов отвечал. И хотя в этих сообщениях не содержалось никакой важной информации, просто шутки, скриншот оказался полезным для них. Они использовали его, чтобы показать, что я связан с сообществом и действительно являюсь одним из его администраторов.

Через некоторое время произошло следующее. Ранее я установил двухступенчатую последовательность идентификации пользователя для

[90] Интервью с Александром, Минск, декабрь 2015, и удалённо из Лондона, апрель 2016.
[91] Имеется в распоряжении Amnesty International.
[92] Интервью с Александром, Минск, декабрь 2015, и удалённо из Лондона, апрель 2016.
[93] Вымышленное имя.

своего аккаунта в «ВКонтакте»: сначала вы вводите пароль, а затем на ваш мобильный телефон приходит сообщение [SMS] с кодом, который вам необходим для доступа к аккаунту. Восемнадцатого декабря я получил 5 сообщений с кодами, которые я не запрашивал. У меня достаточно сложный пароль: он состоит из 18 случайных символов. Я уверен, что его невозможно угадать, и я никогда не записывал его и нигде не хранил, только держал в голове… Что касается второй части идентификации, я думаю, что они получили коды, которые «ВКонтакте» послал на мой мобильный телефон, от Velcom.

Я думаю, что это была не администрация университета, а КГБ. [В ходе последовавшей затем встречи сотрудники университета] распечатали скриншоты моей переписки и пытались меня шантажировать. Вся переписка носила личный характер. Я гей и не скрываю этого. Они пытались использовать эту информацию, унижая меня и оказывая на меня моральное давление с тем, чтобы я начал сотрудничать с ними и передавал им информацию. Они открыто сказали: «будешь сотрудничать с нами, сможешь закончить университет; откажешься – тебя исключат». Они не угрожали опубликовать скриншоты, хотя, как я им и сказал, я вообще не скрываю того, что я гей.

И как они использовали эту информацию – не прямо против меня, но против моей семьи. Мой брат живёт в маленьком городе (райцентре) и работает на государственном заводе. Он был заместителем главного инженера, и когда главный инженер уволился, предполагалось, что мой брат займёт его место. КГБ долго разговаривал с ним по этому поводу (даже с применением полиграфа), и основной темой разговора была моя жизнь и то, что они обо мне знали. Они спросили его о том, чем я занимаюсь, например, о международном финансировании, чтобы выяснить, знает ли он что-нибудь об этих вопросах.

Я бы хотел подчеркнуть, что я вовсе не являюсь самым опасным человеком для этой власти. Я был студенческим активистом, участвовал исключительно в студенческих проектах, и всего один раз организовал встречу. Я не представлял угрозы для безопасности. Я общался с рядом европейских организаций и представлял Беларусь на европейских форумах, и из-за этого меня сочли опасным. И это вовсе не уровень оппозиционных лидеров, таких как Статкевич.[94] По сравнению с этими людьми, я никто. И они применяют по отношению ко мне такие суровые меры».[95]

4.8 КОНФИСКАЦИЯ

В то время как документально подтверждённые случаи взлома данных пользователей, возможно, сравнительно редки, конфискация компьютеров, телефонов и другого оборудования остаётся гораздо более распространённой угрозой для активистов, и в равной степени может обеспечить правительству доступ к персональным данным. Эксперты в области цифровой безопасности, с которыми разговаривала Amnesty International, считают конфискацию устройств наибольшей угрозой информационной безопасности, с которой сталкиваются активисты в Беларуси, и отмечают, что аресты, в результате которых никого не привлекали к суду, тем не менее могли сопровождаться конфискациями.[96]

Одно из последствий конфискации устройств заключается в том, что даже в случае возвращения устройств владельцам, они, как правило, пользуясь ими, больше не чувствуют себя в безопасности. Они опасаются, что их могли каким-нибудь образом взломать, и теперь они могут использоваться для слежки за владельцами.[97]

[94] Оппозиционный политик Николай Статкевич, см. выше раздел «Использование слежки в ходе репрессий, последовавших за выборами 2010 года».
[95] Удалённое интервью с «Иваном», Лондон, апрель 2016.
[96] Интервью с интернет-экспертами, Вильнюс, август 2015.
[97] Интервью с интернет-экспертами, Вильнюс, август 2015.

«ОЧЕВИДНО, ЧТО МЫ УЖЕ НЕ МОЖЕМ БЫТЬ В БЕЗОПАСНОСТИ [ПОСЛЕ КОНФИСКАЦИИ ВЛАСТЬЮ НАШИХ КОМПЬЮТЕРОВ И ИХ ПОСЛЕДУЮЩЕГО ВОЗВРАЩЕНИЯ]… У НАС НЕТ ДЕНЕГ ДЛЯ ТОГО, ЧТОБЫ ОПЛАТИТЬ ЭКСПЕРТА, КОТОРЫЙ ПРОВЕРИТ НАШИ УСТРОЙСТВА, ИЛИ ЧТОБЫ КУПИТЬ НОВОЕ ОБОРУДОВАНИЕ. ТАМ МОГУТ БЫТЬ ШПИОНСКИЕ ПРОГРАММЫ… ПОСЛЕ ТОГО, КАК НАМ ВЕРНУЛИ КОМПЬЮТЕРЫ, МЫ ПО-ПРЕЖНЕМУ ПОЛЬЗОВАЛИСЬ ИМИ, НО МЫ СТАРАЛИСЬ НЕ ИСПОЛЬЗОВАТЬ ИХ ТАК ЖЕ ИНТЕНСИВНО, КАК РАНЬШЕ. МЫ ЗАМЕНИЛИ МНОГИЕ ИЗ НИХ, НО НЕ ВСЕ, ТУТ ВСЁ СНОВА УПИРАЕТСЯ В ДЕНЬГИ».

МОЛОДЁЖНЫЙ АКТИВИСТ, ИНТЕРВЬЮ ПРОВЕДЕНО ДИСТАНЦИОННО ИЗ ЛОНДОНА, МАРТ 2016.

Один из оппозиционных политиков рассказал, как после выборов 2010 года «[Органы государственной власти] конфисковали три компьютера. Потом они вернули их, но ими нельзя было пользоваться, потому что с ними, конечно, что-то делали». Он сказал, что также были конфискованы карты памяти и другие устройства для хранения информации, «и их потом вернули, как бы приглашая нас использовать их, однако я попытался использовать их на компьютере моего друга, на котором он проверяет устройства на наличие вирусов; и они были очень сильно заражены».[98]

Один из студенческих активистов заметил: «Наши ноутбуки конфисковали [в 2010 году], и у нас не было денег, чтобы купить новое оборудование. Совместно с правозащитным центром «Вясна» мы начали осаждать местные отделения КГБ требованиями «Верните наши ноутбуки», «У нас не осталось технического оборудования и поэтому мы не можем работать», «На этих ноутбуках у нас осталось очень много важной информации», «Я не могу закончить свою университетскую курсовую: как мне дальше учиться?» и так далее… Мы намеренно упоминали эту причину, так как в то время я ещё был студентом. Мне вернули ноутбук и компьютер только через три месяца. И у меня больше не было абсолютно никакого желания им пользоваться».[99]

Ещё один активист отметил по поводу конфискации, что «когда мы работаем с спонсорами, это представляет собой очень серьёзную проблему». Он сказал, что это часто связано с необходимостью перевозить крайне важные финансовые и другие документы, заявки на получение финансирования и т.д. - через границы, что создаёт угрозу обнаружения их, в случае если их устройства были бы конфискованы;

[98] Интервью с Андреем Санниковым, Варшава, август 2015.
[99] Интервью со студенческим активистом, Минск, декабрь 2015.

это создаст для них угрозу юридических осложнений, поскольку финансирование незарегистрированной организации может привести к уголовному наказанию.[100]

ЛЕОНИД СУДАЛЕНКО
КОНФИСКАЦИЯ КОМПЬЮТЕРОВ

Правозащитник Леонид Судаленко заявил, что власти много раз конфисковывали компьютеры и другие устройства у него из дома и из офиса:[101]

> «Обыски и конфискации, о которых идёт речь, [см. раздел «Взлом» выше] происходили не впервые. Это был уже второй обыск, проведённый у меня дома, и пятый, устроенный в моём офисе. Они всегда изымали компьютеры, и всегда находили поводы для того, чтобы прийти и конфисковать наше офисное оборудование. Обычно они изымали наши компьютеры, изучали их примерно полгода, и затем возвращали. Некоторые компьютеры возвращали сломанными. Это всегда мешает рабочему процессу…
>
> [Возвращённые после конфискации компьютеры] мы не используем.
>
> И то же самое происходит, когда я пересекаю государственную границу. Например, последний раз это случилось в прошлом году, когда я возвращался в Минск из Вильнюса. Моё имя значилось в их базе данных. Посмотрев мой паспорт, они сразу же уводят меня в другую комнату, обыскивают и обычно забирают мой ноутбук, чтобы вернуть его примерно через шесть месяцев. Но я не буду пользоваться ноутбуком после этого, потому что к этому времени благодаря спонсорской программе у меня уже будет другой. Я имею в виду абсолютно новый, из магазина, запакованный в коробку, который можно использовать без опаски.
>
> Это происходило уже несколько раз, например, в прошлом году это случалось дважды – 24 мая и 25 августа. Оба раза меня тщательно обыскали, даже заставляли снимать носки. И оба раза они начинали обыскивать меня после того, как проверили мой паспорт».[102]

4.9 СКОВЫВАЮЩИЙ ЭФФЕКТ: ЗАКЛЮЧЕНИЕ

Поскольку за многие формы законного активизма в Беларуси предусмотрены уголовные или иные наказания, активисты гражданского общества живут под постоянной угрозой того, что слежка за их личными коммуникациями может подвергнуть их опасности. Непроницаемая завеса секретности, скрывающая применение слежки, и отсутствие соответствующего регулирования и надзора за её применением (см. ниже) означает, что слежка может нарушать права активистов гражданского общества, даже если она не ведётся непосредственно за ними.

Активисты опасаются, что в их офисах установлены «жучки», их телефонные разговоры прослушиваются, их местоположение отслеживается и их онлайн-коммуникациям угрожает взлом. Психологический стресс, который вызван опасениями по поводу слежки, а также возникающая из-за подобных опасений самоцензура подрывают способность активистов заниматься их деятельностью. Самая основная и наиболее важная деятельность активистов – встречи, телефонные звонки, организация общественных протестов, сбор средств – затруднены, что подрывает их возможности нормально функционировать. Гражданское общество в Беларуси оказывается ослабленным в результате слежки и сковывающего эффекта, который порождает страх перед ней.

[100] Интервью с молодёжным активистом, Минск, декабрь 2015.
[101] В отношении одного обыска и конфискации компьютеров в 2001 году организация Судаленко успешно подала иск в Комитет ООН по правам человека, который постановил, что обыск и последующее использование информации из изъятых компьютеров являлось нарушением прав человека, http://www2.ohchr.org/english/bodies/hrc/docs/CaseLaw/CCPR-C-105-D-1226-2003_en.doc .
[102] Удалённое интервью с Леонидом Судаленко, Лондон, май 2016.

5. МЕЖДУНАРОДНОЕ ЗАКОНОДАТЕЛЬСТВО В ОБЛАСТИ ПРАВ ЧЕЛОВЕКА И СЛЕЖКА

Статья 17 Международного пакта о гражданских и политических правах (МПГПП) гласит, что «никто не может подвергаться произвольному или незаконному вмешательству в его личную или семейную жизнь, произвольным или незаконным посягательствам на неприкосновенность его жилища или тайну его корреспонденции», а также что «Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств». Как подчеркнул Верховный комиссар ООН по правам человека, «другие права также могут оказаться затронутыми в результате… перехвата цифровых коммуникаций и сбора личных данных».[103] В их числе право на свободу убеждений и выражение мнений, право на свободу мирных собраний и объединений. Эти права также гарантируются МПГПП, государством-участником которого является Беларусь. Эти права гарантирует также Конституция Беларуси.

Слежка может нарушить права человека, даже если содержание коммуникаций не перехвачено, а также в случае, когда были перехвачены только сопутствующие данные – например, время, характер или местоположение коммуникации (так называемые «метаданные»). Как заметил Верховный комиссар ООН по правам человека, «накопление информации, которую обычно относят к «метаданным», может дать представление о поведении человека, его социальных отношениях, личных предпочтениях и индивидуальности, которое даже превосходит по значимости ту информацию, которую мог бы обеспечить доступ к личным коммуникациям».[104]

В определённых обстоятельствах тайное наблюдение может быть совместимо с обязательствами в области прав человека, и может на самом деле служить важным и полезным инструментом в руках правоохранительных органов. Однако там, где национальная правовая база *как таковая* не может быть чётко определена или доступна общественности, или по каким-либо иным причинам не обеспечивает адекватные гарантии безопасности против злоупотреблений, а также там, где цели и характер слежки противоречит международным обязательствам государства в области прав человека, - в этих случаях слежка будет равноценна «произвольному и незаконному» посягательству на неприкосновенность частной жизни или иным образом будет нарушать права человека.

Требования о том, что вмешательство в право на неприкосновенность частной жизни путём слежки за коммуникациями должно соответствовать международным правовым стандартам, суммированы Верховным комиссаром ООН по правам человека следующим образом:

> «Начнём с того, что любое ограничение прав на неприкосновенность частной жизни, закреплённых в статье 17 [МПГПП], должно происходить в соответствии с законом, и это законодательство должно быть доступным, ясно и точно сформулированным, чтобы человек мог обратиться к закону и выяснить, кто именно уполномочен осуществлять слежку за данными и при каких обстоятельствах. Ограничение этих прав должно являться необходимым для достижения законной цели, а также являться соразмерным этой цели, при этом вмешательство должно быть насколько возможно минимальным. Более того, если ограничение осуществляется на основании права (например, вторжение в частную жизнь в целях обеспечения национальной безопасности или в целях защиты права на жизнь других людей), должно быть продемонстрировано, что имеется вероятность достижения поставленных целей. Власти, добивающиеся ограничения этого права, обязаны в данном случае доказать, что данное ограничение преследует законную цель. Далее, любое ограничение права на неприкосновенность частной жизни не должно обессмысливать суть данного права, и должно соответствовать другим правам человека, в том числе запрету на дискриминацию. Если ограничение не соответствуют этим критериям, оно будет являться незаконным, и/или

[103] Верховный комиссар ООН по правам человека, «Право на неприкосновенность частной жизни в цифровую эпоху», A/HRC/27/37, 30 июня 2014 (здесь и далее ВКПЧ ООН «Неприкосновенность частной жизни в цифровую эпоху»), пар. 14.
[104] ВКПЧ ООН «Неприкосновенность частной жизни в цифровую эпоху», пар. 19.

посягательство на неприкосновенность права на частную жизнь будет носить произвольный характер».[105]

105 ВКПЧ ООН «Неприкосновенность частной жизни в цифровую эпоху», пар. 23.

6. СЛЕЖКА ЗА КОММУНИКАЦИЯМИ В БЕЛАРУСИ: ЗАКОНЫ И ПРАКТИКА

4 декабря 2015 года Большая палата Европейского суда по правам человека (ЕСПЧ) вынесла решение по делу *Роман Захаров против России*, постановив, что российская система тайного наблюдения противоречит статье 8 Европейской конвенции о защите прав человека, защищающей право на частную и семейную жизнь. Хотя Беларусь не является участницей Европейской конвенции о защите прав человека, у белорусской и российской системы слежки, ставшей предметом дела Захарова, есть весьма много общего, поэтому решение по этому делу служит полезным ориентиром при анализе воздействия белорусской системы на права человека, особенно с учётом того, что права, о которых шла речь в деле Захарова, также защищаются договорами, участницей которых является Беларусь, в том числе Международным пактом о гражданских и политических правах. Кроме того, многие другие международные эксперты и органы критиковали аспекты режима, регулирующего слежку в Беларуси.

6.1 ПРЯМОЙ ДОСТУП К ДАННЫМ КОММУНИКАЦИЙ

В деле Захарова ЕСПЧ критиковал действующую в России систему, которая даёт властям технические возможности получать прямой доступ к информации и данным[106] без необходимости предъявлять разрешение суда компании-оператору услуг связи. Суд отметил: «по мнению Суда, такая система, как российская, которая позволяет спецслужбам и полиции непосредственно перехватывать коммуникации каждого гражданина без предъявления оператору услуг связи либо кому-то ещё санкции на такой перехват, особо располагает к произволу»[107].

[106] Данные, о которых шла речь в решении по делу Захарова, относятся к переговорам по мобильному телефону.
[107] ЕСПЧ, «Роман Захаров против России», жалоба № 47143/06 (Большая палата), 4 декабря 2015 г., п. 270 (далее дело Захарова); см. также Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение Франка Ла Рю, A/HRC/23/40, п. 61 (2013), (далее A/HRC/23/40) http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

ЧТО ТАКОЕ СОРМ?

СОРМ — это система технических средств для обеспечения оперативно-розыскных мероприятий, то есть стандартизированные технические средства перехвата коммуникаций и относящихся к ним данных. Впервые СОРМ появилась в России и ныне её версии существуют во многих странах бывшего СССР, в том числе в Беларуси, где она обеспечивает государству прямой автоматический доступ к коммуникациям и относящимся к ним данным от операторов услуг связи, в том числе к стационарным телефонам, мобильным сетям и интернет-провайдерам.

Требования и возможности СОРМ в Беларуси изложены главным образом в указе президента № 129 от 2010 года и в технической документации, выработанной и одобренной Министерством связи и информатизации по согласованию с Комитетом государственной безопасности (КГБ) и Оперативно-аналитическим центром при президенте (ОАЦ) согласно статье 6 этого указа.[108]

Согласно закону, операторы должны обеспечивать функционирование СОРМ при построении сети электросвязи, вводе в эксплуатацию новых средств связи и модернизации средств электросвязи.[109] Операторы за счёт собственных средств осуществляют приобретение, установку, техническое обслуживание и ремонт СОРМ.[110]

Операторы должны предоставлять уполномоченным органам безвозмездный круглосуточный удалённый доступ к базам данных об абонентах. Они должны создавать и поддерживать базы данных, к которым у властей есть удалённый доступ, с информацией, идентифицирующей абонентов и их устройства, а также об услугах электросвязи, активированных абонентом.[111] Согласно закону, эта информация хранится пять лет, а относящаяся к СОРМ техническая документация указывает на то, что данные об абонентах и используемых ими услугах может храниться до десяти лет.[112] Подключённые к СОРМ устройства в местах общего доступа (интернет-кафе и проч.) также должны хранить статистические данные в течение 14 дней.

Операторы обеспечивают ограничение доступа своих сотрудников к СОРМ и защищают сведения о тактике проведения оперативно-розыскных мероприятий.[113] Средства СОРМ не допускают неавторизованный доступ к базам данных и не должны оставлять следов удалённого поиска в журналах операторов.[114]

Требования СОРМ незначительно отличаются в зависимости от вида сети (стационарной, мобильной, интернет и проч.), однако у них есть общие черты. СОРМ позволяет вести два вида наблюдений: «полное наблюдение» и «статистическое наблюдение». Как правило, «статистическое» наблюдение касается метаданных связи (вида переданных данных, время использование и т.п.). Полное наблюдение, как правило, предусматривает удалённый доступ ко всей информации пользователя в реальном времени. Наблюдение может быть инициировано по поиску различных видов идентифицирующей информации, например, IP адреса, адреса электронной почты, регистрации пользователя в системе, номера телефона, времени подключения, адресов IMEI,[115] IMSI,[116] MAC[117] и другой информации, с помощью которой можно определить устройство связи. Применительно к мобильным устройствам системы удалённого контроля также позволяют следить за местоположением устройства в определённые интервалы времени либо по требованию. В целом, согласно требованиям стандартов, власти должны иметь возможность начать слежку в течение 30 секунд после отправки команды инициализации.[118]

[108] Указ Президента Республики Беларусь от 3 марта 2010 г. № 129 «Об утверждении Положения о порядке взаимодействия операторов электросвязи с органами, осуществляющими оперативно-розыскную деятельность», http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm.
[109] Указ Президента Республики Беларусь от 3 марта 2010 г. № 129 «Об утверждении Положения о порядке взаимодействия операторов электросвязи с органами, осуществляющими оперативно-розыскную деятельность», статьи 5 и 13, http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm.
[110] Указ Президента Республики Беларусь от 3 марта 2010 г. № 129 «Об утверждении Положения о порядке взаимодействия операторов электросвязи с органами, осуществляющими оперативно-розыскную деятельность», статья 10, http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm.
[111] Указ Президента Республики Беларусь от 3 марта 2010 г. № 129 «Об утверждении Положения о порядке взаимодействия операторов электросвязи с органами, осуществляющими оперативно-розыскную деятельность», статьи 15 и 17, http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm.

В Беларуси прямой доступ к коммуникациям и связанным с ними данным обеспечивается посредством системы, весьма схожей с применяемой в России — системы СОРМ.[119] СОРМ обеспечивает круглосуточный прямой автоматический доступ к данным коммуникаций, хранящимся у интернет-провайдеров и операторов услуг мобильной связи.[120] Новые операторы, получившие лицензию на деятельность в области связи, обязаны в течение месяца письменно сообщить об этом в КГБ и Оперативно-аналитический центр (ОАЦ) при президенте для принятия ими решения о внедрении СОРМ.[121] Согласно закону, при построении сети электросвязи операторы должны обеспечивать внедрение и эксплуатацию СОРМ.[122] Кроме того, операторы за счёт собственных средств осуществляют приобретение, установку, и техническое обслуживание СОРМ, защиту сведений о тактике проведения оперативно-розыскных мероприятий, ограничение круга лиц, привлекаемых к установке и техническому обслуживанию СОРМ.[123] При отсутствии технической возможности организации удалённого доступа к базам данных абонентов по письменному обращению оператор обязан передать копию баз данных абонентов на материальных носителях информации в КГБ, Министерство внутренних дел или ОАЦ.[124]

Белорусское законодательство не требует предъявлять операторам электросвязи какие-либо документы, санкционирующие доступ к данным коммуникаций.

В Беларуси нет общедоступной информации о том, как часто власти пользуются доступом к коммуникациям или связанным с ними данным. В ответ на просьбу Amnesty International предоставить эти статистические данные Департамент финансовых расследований Комитета государственного контроля заявил, что такие данные предоставить невозможно за их отсутствием, а также по той причине, что «некоторая информация, согласно законодательству Республики Беларусь, определяется как государственная тайна».[125]

6.2 ХРАНЕНИЕ ДАННЫХ

В решении по делу Захарова ЕСПЧ отметил, что Суд Европейского союза (Суд ЕС) недавно критиковал директивы о всеохватном хранении данных — в решении от 8 апреля 2014 года по совместному делу *Digital Rights Ireland and Seitinger and Others*. Суд ЕС признал недействительной Директиву ЕС о хранении данных (2006/24/EC), которая требовала от операторов публичных услуг электронной связи либо публичных сетей связи хранить все данные о трафике и местоположении, но не содержание коммуникаций, от шести месяцев до двух лет. Суд ЕС признал, что хранение данных представляет собой серьёзное и масштабное нарушение основных прав, особенно права на частную жизнь, и отметил: «тот факт, что данные хранятся и впоследствии используются без уведомления абонента или зарегистрированного пользователя, с большой вероятностью вызовет у данных лиц ощущение того, что их частная жизнь постоянно находится под наблюдением».[126]

---

[112] Сети электросвязи СИСТЕМА ТЕХНИЧЕСКИХ СРЕДСТВ ДЛЯ ОБЕСПЕЧЕНИЯ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ Технические требования (копия имеется у Amnesty International). Неясно, являются ли эти технические требования последней текущей версией. Amnesty International запрашивала подтверждение у ряда органов белорусского правительства, но ответа не получила.

[113] Указ Президента Республики Беларусь от 3 марта 2010 г. № 129 «Об утверждении Положения о порядке взаимодействия операторов электросвязи с органами, осуществляющими оперативно-розыскную деятельность», статья 10, http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm.

[114] Сети электросвязи СИСТЕМА ТЕХНИЧЕСКИХ СРЕДСТВ ДЛЯ ОБЕСПЕЧЕНИЯ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ Технические требования (копия имеется у Amnesty International).

[115] International Mobile Equipment Identity (международный идентификатор аппаратуры мобильного оборудования): номер, позволяющий идентифицировать мобильный телефон.

[116] International Mobile Subscriber Identity (международный идентификатор абонента мобильной связи): номер, позволяющий идентифицировать абонента мобильной связи.

[117] Аппаратный адрес: уникальный постоянный идентификатор устройства, присваиваемый сетевой плате компьютера при сборке.

[118] Сети электросвязи СИСТЕМА ТЕХНИЧЕСКИХ СРЕДСТВ ДЛЯ ОБЕСПЕЧЕНИЯ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ Технические требования (копия имеется у Amnesty International).

[119] Система технических средств для обеспечения оперативно-розыскных мероприятий, см. Указ Президента Республики Беларусь от 3 марта 2010 г. № 129 «Об утверждении Положения о порядке взаимодействия операторов электросвязи с органами, осуществляющими оперативно-розыскную деятельность», статья 2, http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm.

[120] Указ Президента Республики Беларусь от 3 марта 2010 г. № 129 «Об утверждении Положения о порядке взаимодействия операторов электросвязи с органами, осуществляющими оперативно-розыскную деятельность», статья 15, http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm.

[121] Указ Президента Республики Беларусь от 3 марта 2010 г. № 129 «Об утверждении Положения о порядке взаимодействия операторов электросвязи с органами, осуществляющими оперативно-розыскную деятельность», статья 7, http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm.

[122] Указ Президента Республики Беларусь от 3 марта 2010 г. № 129 «Об утверждении Положения о порядке взаимодействия операторов электросвязи с органами, осуществляющими оперативно-розыскную деятельность», статья 5, http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm.

[123] Указ Президента Республики Беларусь от 3 марта 2010 г. № 129 «Об утверждении Положения о порядке взаимодействия операторов электросвязи с органами, осуществляющими оперативно-розыскную деятельность», статья 10, http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm.

[124] Согласно статье 17 указа об оперативно-розыскной деятельности, базы данных об абонентах включают: 1) абонентский номер, фамилию, имя, отчество, адрес абонента и другие данные, позволяющие идентифицировать абонента, а для абонентов мобильной связи также требуется абонентский номер; 2) общие сведения об услугах электросвязи, активированных абонентом. Указ Президента Республики Беларусь от 3 марта 2010 г. № 129 «Об утверждении Положения о порядке взаимодействия операторов электросвязи с органами, осуществляющими оперативно-розыскную деятельность», статьи 16 и 17, http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm.

[125] Письмо из Департамента финансовых расследований Комитета государственного контроля, 3 июня 2016 г. (копия имеется у Amnesty International).

[126] Дело «Digital Rights Ireland and Seitinger and Others» (C-293/12 и C-594/12), Суд Европейского союза, 8 апреля 2014 года, п. 37; см. также УВКПЧ ООН, «Право на неприкосновенность личной жизни в цифровой век», п. 26 («Не может считаться необходимой или соразмерной практика обязательного сохранения данных третьей стороны — стандартная практика слежения во многих странах, где правительства обязывают телефонные компании и компании, поставляющие интернет-услуги, хранить метаданные о контактах и местоположении клиентов для последующего использования в рамках правоохранительной деятельности, равно как и для предоставления разведывательным агентствам»); см. также A/HRC/23/40, п. 67.

В Беларуси поставщики услуг связи обязаны хранить многие виды данных пользователей. Например, указ президента № 60 от 2010 года обязывает поставщиков интернет-услуг идентифицировать абонентские устройства, а также сведения об оказанных интернет-услугах. Аналогично, согласно постановлению Совета министров № 1055 от 2006 года, интернет-провайдеры в течение года должны хранить информацию, идентифицирующую абонентов (в том числе адреса MAC и IP[127], время соединения, а также домены и IP-адреса ресурсов, запрошенных пользователями).[128] Информация об оказанных услугах и оплаченных счетах хранится в течение пяти лет.[129] По состоянию на 1 января 2016 года, согласно постановлению № 6 Министерства связи от 18 февраля 2015 года, поставщики интернет услуг должны хранить аналогичные категории данных с целью идентификации пользователей и их действий в интернете в течение года.[130]

Аналогичным образом собственники пунктов коллективного пользования интернетом (например, интернет-кафе) должны вести учёт и хранение персональных данных пользователей, а также сведений об интернет-услугах. Эта информация должна храниться в течение года и предоставляться «по требованию органов, осуществляющих оперативно-розыскную деятельность, органов прокуратуры и предварительного следствия, органов Комитета государственного контроля, налоговых органов, судов в порядке, установленном законодательными актами».[131] Однако требования постановления Совета министров № 1055 от 2006 года о хранении владельцами абонентских номеров пользователей были смягчены постановлением № 1191 от 2012 года, которое допускает и другие средства, например, фотографирование и видеозаписи в помещении либо регистрацию абонентов по СМС.

Технические требования к базам данных СОРМ требуют от операторов хранить многие категории данных пользователей[132] до десяти лет. Власти могут получить доступ к этим данным в удалённом режиме.

6.3 СФЕРА ПРИМЕНЕНИЯ МЕР ТАЙНОГО НАБЛЮДЕНИЯ

В решении по делу Захарова ЕСПЧ подчеркнул, что национальные законы должны соответствующим образом предусматривать обстоятельства, в которых могут применяться полномочия слежки. ЕСПЧ выразил тревогу, что слежку могут вести не только за подозреваемым в соответствии с российским законодательством, но также за «лицом, у которого может иметься информация об уголовном преступлении» либо за «лицом, у которого может быть информация, относящаяся к уголовному делу», причём ни то, ни другое не определяется законодательством.[133]

Кроме того, суд выразил тревогу, что слежка обосновывается неопределёнными обстоятельствами, в том числе необходимостью защиты национальной, экономической и экологической безопасности, однако российское законодательство никак не определяет эти угрозы, что создаёт возможности для произвола.[134]

В Беларуси слежка санкционируется в рамках Уголовно-процессуального кодекса (далее УПК) либо законом «Об оперативно-розыскной деятельности» (далее закон ОРД).[135] Согласно статье 214 УПК, прослушивание и запись переговоров ограничиваются уголовными делами о тяжких и особо тяжких преступлениях. Однако такие действия применяются не только в отношении подозреваемых, но и «других лиц», если имеются достаточные основания полагать, что переговоры могут содержать сведения, имеющие значение для дела.[136]

Согласно закону ОРД, слежка проводится по множеству оснований, из которых целый ряд определяется довольно широко и расплывчато, в том числе, если имеются:

- «сведения о событиях и действиях, создающих угрозу национальной безопасности Республики Беларусь;

---

[127] Уникальный адрес, идентифицирующий адрес в интернете или локальной сети.
[128] Постановление Совета министров Республики Беларусь от 17.08.2006 № 1055, п. 181, http://naviny.org/2006/08/17/by38581.htm. Неспособность сохранить эту информацию считается «характерным нарушением» лицензионных требований Министерства связи, http://www.mpt.gov.by/ru/new_page_5_6_15100/
[129] Постановление Совета министров Республики Беларусь от 17.08.2006 № 1055, п. 146, http://naviny.org/2006/08/17/by38581.htm.
[130] Постановление Министерства связи № 6 от 18 февраля 2015 г., п. 3, http://www.belgie.by/_files/npa/p_min_sv_i_inf_n_6.doc; см. также http://www.mpt.gov.by/ru/content/3632. В то время как постановление № 6 последовало за указом Президента Республики Беларусь от 28 декабря 2014 г. № 6 «О неотложных мерах по противодействию незаконному обороту наркотиков», в законодательстве не существует однозначного требования об ограничении использования данных целями борьбы с незаконным оборотом наркотиков.
[131] Указ Президента Республики Беларусь № 60 от 2010 «О мерах по совершенствованию использования национального сегмента сети Интернет», статья 6 [неофициальный перевод] http://www.e-belarus.org/docs/decree60.html
[132] См. «Что такое СОРМ?»
[133] Дело Захарова, п.п. 243-249.
[134] См. также A/HRC/23/40, п. 83 («Правовая база должна обеспечивать, чтобы меры по слежению за сообщениями: (a) были предписаны законом и удовлетворяли нормам ясности и чёткости, что является достаточным для обеспечения того, чтобы частные лица были заблаговременно уведомлены о них и могли предвидеть их применение».)
[135] Закон от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности», http://kgb.by/ru/zakon289-3/
[136] Уголовно-процессуальный кодекс, статья 214.

- сведения о подготавливаемом или совершаемом преступлении, а также о гражданине, его подготавливающем, совершающем или совершившим либо осведомлённом о нём; [или]
- поручение, указание, постановление органа уголовного преследования по уголовному делу, рассматриваемому заявлению или сообщению о преступлении».[137]

По всей видимости, законодательство никак не поясняет и не суживает большинство этих оснований. Единственным исключением является понятие национальной безопасности, которое определяется указом президента. Тем не менее, определение, содержащееся в этом указе, настолько широко, что практически не служит руководством в вопросе о том, когда допускается законно обоснованная слежка.[138]

Компании, от которых не требуется внедрение СОРМ для доступа правительства к данным, например, отечественных операторов услуг электронной почты, предоставляющих хостинг иностранным поставщикам услуг электронной почты, также могут заставить предоставить данные пользователей на основании запроса прокуратуры. По меньшей мере один провайдер отметил, что такие запросы поступают регулярно и в целом представляют собой требования предоставить имена пользователей и пароли, и таким образом власти получают полный доступ к учётной записи пользователя, не ограничиваясь датами, темами или конкретной корреспонденцией.[139]

6.4 ОТКРЫТОСТЬ ВНУТРЕННЕГО ЗАКОНОДАТЕЛЬСТВА

Что касается российской системы СОРМ, о которой шла речь в деле Захарова, технические требования к установке аппаратуры наблюдения операторами, описаны в приложении к указу № 70 Министерства связи. Поскольку эти технические требования могут отразиться на праве пользователей на частную и семейную жизнь, ЕСПЧ призвал их опубликовать.[140]

В Беларуси технические требования СОРМ вырабатываются и утверждаются Министерством связи и информатизации по согласованию с КГБ и ОАЦ по статье 6 указа президента № 129 от 2010 года. Эти требования, по всей видимости, не являются общедоступными.[141]

6.5 САНКЦИОНИРОВАНИЕ МЕР НАБЛЮДЕНИЯ

В решении по делу Захарова ЕСПЧ отметил, что российское требование судебной санкции на слежку является важной мерой защиты от произвола. Однако эту меру защиты подрывает ряд проблем, в том числе отсутствие требования к судьям проверять наличие разумных подозрений, а также необходимость и соразмерность этих мер. Кроме того, ЕСПЧ выразил тревогу в связи с отсутствием предусмотренного законом требования об указании конкретного лица или номера телефона в качестве объекта слежки. Суд также критиковал тот факт, что в «неотложных» случаях для начала слежки не требуется санкция суда и что рассмотрение санкции в суде после последующего уведомления ограничивается лишь вопросом о продлении этой санкции, а не о том, была ли обоснована первоначальная санкция, либо о том, следует ли хранить или уничтожить собранные данные.[142]

В Беларуси, согласно статье 19 закона ОРД, ряд видов оперативно-розыскных мероприятий, включая установку средств негласного наблюдения, прослушивающих устройств и контроль в сетях электросвязи или почтовых отправлений, требуют санкции прокурора или его заместителя, но не судьи.

Многочисленные органы могут запрашивать санкцию на проведение оперативно-розыскных мероприятий, что в рамках закона ОРД включает различные формы негласного наблюдения. А именно: органы внутренних дел, органы государственной безопасности, органы пограничной службы, Служба безопасности президента Республики Беларусь, Оперативно-аналитический центр при президенте Республики Беларусь,

---

[137] Закон от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности», п. 16, http://kgb.by/ru/zakon289-3/

[138] http://naviny.org/2010/11/09/by18748.htm Указ Президента Республики Беларусь № 575 от 2010 г. «закрепляет совокупность официальных взглядов на сущность и содержание» концепции национальной безопасности. Это объёмный и крайне обширный документ. Например, в пункте 27, главы 4 перечислены 30 отдельных видов «угроз национальной безопасности». Некоторые из этих угроз касаются темы терроризма, однако в перечне также содержатся такие пункты, как «снижение уровня благосостояния и качества жизни населения», «рост безработицы», «недостаточные объёмы и низкое качество иностранных инвестиций», а также «попытки разрушения национальных духовно-нравственных традиций и необъективного пересмотра истории».

[139] Беседа с белорусским оператором услуг электронной почты, Минск, 2015 год.

[140] Дело Захарова, п. 241; см. также A/HRC/23/40, п. 91, («Государства должны демонстрировать полную транспарентность в отношении применения и охвата методов и полномочий слежения».)

[141] Указ Президента Республики Беларусь от 3 марта 2010 г. № 129 «Об утверждении Положения о порядке взаимодействия операторов электросвязи с органами, осуществляющими оперативно-розыскную деятельность», статья 6, http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm; Amnesty International просила белорусские власти пояснить этот пункт, однако ответа не получила.

[142] Дело Захарова, п.п. 57-67.

органы финансовых расследований Комитета государственного контроля, таможенные органы Республики Беларусь, разведывательные службы Вооружённых сил Республики Беларусь.[143]

Органы, осуществляющие оперативно-розыскные мероприятия, направляют письменный запрос об их проведении прокурору или его заместителю и представляют документы, содержащие основания для проведения оперативно-розыскного мероприятия. Прокурор или его заместитель при даче санкции указывают срок, в течение которого оно может быть проведено. При отказе должностное лицо органа, осуществляющего оперативно-розыскную деятельность, вправе обратиться по этому вопросу к вышестоящему прокурору.[144]

Согласно статье 214 Уголовно-процессуального кодекса, прослушивание и запись переговоров допускается с санкции прокурора или его заместителя либо председателей Следственного комитета или Комитета государственной безопасности (КГБ).[145]

При этом закон не требует от прокуроров, санкционирующих такие методы, проверять наличие разумных оснований либо необходимости и соразмерности, а также указывать конкретное лицо или адрес в качестве объекта слежки.

В Беларуси также существуют целый ряд обстоятельств, при которых для ведения слежки не требуется даже санкции прокурора. Статья 35 закона ОРД гласит, что оперативно-розыскное мероприятие, обычно требующее санкции прокурора или его заместителя, может санкционироваться постановлением министра внутренних дел либо председателя Комитета государственной безопасности или его заместителя в случаях, «не терпящих отлагательства, для предупреждения, выявления, пресечения тяжкого или особо тяжкого преступления, розыска и задержания гражданина, его совершившего, а также при наличии сведений о событиях и действиях, создающих угрозу национальной безопасности Республики Беларусь».

Согласно статье 37 закона ОРД, оперативно-розыскные мероприятия могут проводиться без санкции прокурора или его заместителя при условии письменного уведомления в течение 24 часов и получения санкции на него в течение 48 часов «в случаях, не терпящих отлагательства, для предупреждения, выявления, пресечения тяжкого или особо тяжкого преступления, розыска и задержания гражданина, его совершившего, для предупреждения действий, которые могут привести к уничтожению предметов и документов, которые могут быть признаны вещественными доказательствами, а также при наличии сведений о событиях и действиях, создающих угрозу национальной безопасности Республики Беларусь».

Согласно статье 38, оперативно-розыскные мероприятия, в том числе установка средств слухового контроля, контроль почтовых отправлений и контроль в системах телекоммуникаций в здании, транспортном средстве и ином объекте допускается без санкции прокурора или его заместителя по заявлению гражданина или с его согласия в письменной форме либо по заявлению его близкого, опекуна или попечителя о возникновении угрозы его жизни, здоровью и сохранности имущества. В таких случаях прокурора или его заместителя следует уведомить об этом в письменном виде в течение 48 часов.

6.6 НАДЗОР ЗА МЕРАМИ НАБЛЮДЕНИЯ

В решении по делу Захарова ЕСПЧ выразил тревогу отсутствием достаточного надзора за мерами наблюдения с целью предотвращения произвола. У суда вызвал беспокойство тот факт, что система СОРМ не предусматривает журналов учёта розыскных действий, что лишает надзорные органы главного средства выявления несанкционированной слежки. ЕСПЧ отметил, что в России вопрос о достаточности прокурорского надзора зависит от прокурорских полномочий и компетентности, а также независимости от органов, ведущих наблюдение. ЕСПЧ установил, что независимость прокуроров подрывает тот факт, что они назначаются и снимаются с должности генеральным прокурором. Далее ЕСПЧ отметил, что «слияние функций в рамках одной прокуратуры, при котором один и тот же орган санкционирует перехват информации, а затем ведёт за этим надзор, […] также может вызвать сомнения в независимости прокуроров». ЕСПЧ отметил, что надзорным органам должны быть доступны все соответствующие документы, они должны обладать полномочиями, позволяющими устранять нарушения и должны быть открыты надзору, например, посредством публикации отчётов о своих надзорных функциях. Кроме того, суд счёл, что власти не предоставили примеров практических действий прокуроров по устранению нарушений.[146]

---

[143] Закон от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности», статья 12, http://kgb.by/ru/zakon289-3/
[144] Закон от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности», статья 19, http://kgb.by/ru/zakon289-3/
[145] УПК, статья 214.
[146] Дело Захарова, п.п. 272 – 285. См. также A/HRC/23/40, п. 86, («Предоставление коммуникационных данных государствам должно контролироваться независимым органом, таким как суд или надзорный механизм».)

В Беларуси прокурорам предоставлены определённые полномочия по надзору за оперативно-розыскными мероприятиями и расследованиями, однако закон не обязывает их пользоваться этими полномочиями. Например, они могут получить доступ к оперативным материалам, потребовать объяснений, отменить оперативно-розыскные мероприятия или даже в случае нарушений принять дисциплинарные меры или возбудить уголовное дело.[147] Информация об обращениях к базам данных СОРМ хранится пять лет, но хранится она самими уполномоченными подразделениями, а не прокурорами.[148] Как отметил Европейский суд по правам человека, в России отсутствие информации лишает прокуроров главного средства выявления нарушений. Кроме того, как и в России, прокуроры назначаются и снимаются с должности генеральным прокурором, которого в Беларуси назначает Национальное собрание.[149] Кроме того, тот факт, что прокуроры санкционируют и ведут надзор за мерами наблюдения, потенциально вызывает конфликт интересов. В целом, прокуратура, по всей видимости, не публикует отчётов или данных о своих надзорных функциях.

6.7 ПРОДОЛЖИТЕЛЬНОСТЬ ТАЙНОГО НАБЛЮДЕНИЯ

В решении по делу Захарова ЕСПЧ подчеркнул, что для гарантии защиты от произвольной слежки в законе должен быть чётко прописан срок, по истечении которого ордер на перехват информации утрачивает силу, а также обстоятельства, позволяющие продлить действие такого ордера, и обстоятельства, требующие отмены ордера.[150]

Поскольку в России третий критерий выполняется лишь применительно к уголовным делам, а не к делам, касающимся национальной безопасности, достаточные гарантии защиты в стране не существуют.

Статья 214 белорусского Уголовно-процессуального кодекса гласит: «О необходимости осуществления прослушивания и записи переговоров… орган дознания выносит мотивированное постановление, в котором указываются уголовное дело и основания… и в течение какого срока.

Прослушивание и запись переговоров в любом случае не могут осуществляться свыше срока предварительного расследования уголовного дела и отменяются постановлением следователя, органа дознания».

Таким образом, хотя прослушивание по данной статье должно прекратиться по завершении предварительного следствия, статья не определяет ни возможную продолжительность прослушивания, ни необходимость продления соответствующего постановления.

Согласно статье 19 закона ОРД, прокурор или его заместитель при даче санкции указывают срок, в течение которого может быть проведено оперативно-розыскное мероприятие. Согласно статье 41, в ряде определённых случаев этот срок не должен превышать 90 дней, включая слуховой контроль и контроль в сетях электросвязи, а в иных случаях составляет до 180 дней.

Статья 43 предусматривает, что применительно к большинству видов наблюдения их срок может продляться на основании мотивированного постановления до 180 суток прокурорами областей, города Минска или их заместителями, до 365 суток заместителем генерального прокурора Республики Беларусь и до 545 суток генеральным прокурором Республики Беларусь.

Статья 46 требует прекращения оперативно-розыскного мероприятия в отсутствие оснований для дальнейшего его проведения либо по истечении срока его проведения.

Таким образом, хотя закон ОРД требует устанавливать сроки мер наблюдения, эти меры довольно длительны. В случае продления срока слежка может продолжаться до полутора лет, причём согласие судьи для этого не требуется.

6.8 ОБРАЩЕНИЕ С ДАННЫМИ

[147] Закон Республики Беларусь «О прокуратуре Республики Беларусь», http://www.pravo.by/webnpa/text.asp?&p0=H10700220; статьи 69 и 70 закона ОРД также предусматривают надзор за оперативно-розыскными мероприятиями со стороны прокуроров, а также контроль за ними руководителей осуществляющих их органов, закон от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности», http://kgb.by/ru/zakon289-3/

[148] Указ Президента Республики Беларусь от 3 марта 2010 г. № 129 «Об утверждении Положения о порядке взаимодействия операторов электросвязи с органами, осуществляющими оперативно-розыскную деятельность», статья 15, http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm

[149] Закон Республики Беларусь «О прокуратуре Республики Беларусь», статьи 13-14, http://www.pravo.by/webnpa/text.asp?&p0=H10700220

[150] Дело Захарова, п.п. 250-252; см. также A/HRC/23/40, п. 81 («В законе должны быть чётко прописаны гарантии, касающиеся… продолжительности возможных мер слежения».)

В решении по делу Захарова ЕСПЧ отметил, что закон должен предусматривать достаточные гарантии касательно хранения, доступа, рассмотрения, использования, обмена и уничтожения данных. Применительно к России суд отметил ряд вызывающих тревогу вопросов, особенно отсутствие требования о немедленном уничтожении данных, не относящихся к целям, с которыми их собирали, неограниченную свободу действий судей в том что касается уничтожения данных, использующихся в качестве доказательства, по завершении судебного разбирательства.

В Беларуси статьи 14 и 50 закона ОРД требуют от органов, осуществляющих оперативно-розыскную деятельность, не разглашать и не использовать во вред гражданам сведения, затрагивающие неприкосновенность частной жизни. Органы, осуществляющие оперативно-розыскную деятельность, могут предоставлять в другой орган или международную организацию информацию, собранную в результате оперативно-розыскных мероприятий. Однако угроза сохранению в тайне личных сведений о гражданах может послужить основанием для отказа в предоставлении таких материалов.

Согласно статье 14 закона ОРД, власти должны уничтожать материалы оперативно-розыскной деятельности, содержащие сведения, не связанные с противоправной деятельностью. Однако никакие конкретные сроки в этой связи не указаны и не упоминается, когда должны уничтожаться материалы оперативно-розыскных мероприятий, связанные с противоправной деятельностью, например, по завершении судебного разбирательства.

6.9 УВЕДОМЛЕНИЕ О НАБЛЮДЕНИИ

В решении по делу Захарова ЕСПЧ отметил, что требование об уведомлении лиц о том, что за ними велось наблюдение, «неразрывно связано с эффективностью средств судебно-правовой защиты». Признав, что соблюдение секретности порой является ключевой составляющей слежки, суд тем не менее отметил: «Как только уведомление становится возможным без риска для цели ограничения по завершении мер наблюдения, информация об этом должна быть предоставлена всем заинтересованным лицам».[151]

Законодательство Беларуси не требует уведомлять о слежке подвергающихся ей лиц. Это особенно проблематично с учётом того, что у правительства есть прямой доступ к сообщениям и связанным с ними данными через СОРМ, от него не требуется уведомлять провайдеров об этом доступе, и информация об оперативно-розыскной деятельности в целом должна оставаться конфиденциальной.[152]

Даже в ситуациях, когда операторам предъявляют соответствующую санкцию, например, в случае провайдеров услуг электронной почты, недоступных для СОРМ, закон запрещает им разглашать информацию о доступе к данным.[153]

Однако лицо, узнавшее о том, что оно находилось под наблюдением, и считающее, что его права оказались нарушены, вправе потребовать от органов, осуществляющих оперативно-розыскную деятельность, раскрыть информацию при условии, что в отношении него в возбуждении уголовного дела отказано или судом вынесен оправдательный приговор. Однако в предоставлении этой информации также может быть отказано, если основания для отказа утверждены судом.[154]

Как отметил ЕСПЧ в отношении весьма схожего порядка уведомлений в России, учитывая ограничения касательно раскрытия информации и тот факт, что «заинтересованное лицо, скорее всего, никогда не узнает о перехвате своих сообщений», такой порядок уведомлений о наблюдении не является эффективным.[155]

6.10 СРЕДСТВА ПРАВОВОЙ ЗАЩИТЫ

Нормы международного права в области прав человека требуют предоставлять средства судебно-правовой защиты лицам, чьи права оказались нарушены.[156] В Беларуси теоретически существует несколько

---

[151] Дело Захарова, п.п. 286-7; см. также A/HRC/23/40, п. 82, («Учитывая, что заблаговременное или совпадающее по времени уведомление может поставить под угрозу эффективность слежения, частные лица должны, тем не менее, уведомляться об этом сразу же после окончания слежения. Они также должны иметь возможность добиться возмещения ущерба в связи с применением к ним мер по слежению за сообщениями после их завершения».)
[152] Закон от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности», статьи 8 - 10, http://kgb.by/ru/zakon289-3/
[153] Статья 407 Уголовного кодекса запрещает разглашение данных расследования.
[154] Закон от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности», п.п. 14.16 и 14.21, http://kgb.by/ru/zakon289-3/
[155] Дело Захарова, п. 289.
[156] Например, см. статью 2 МПГПП: «3. Каждое участвующее в настоящем Пакте Государство обязуется:

правовых механизмов возмещения ущерба, причинённого нарушением прав в связи со слежкой. Однако, как отмечается ниже, многие из тех, с кем беседовала Amnesty International, не спешат воспользоваться этими механизмами по ряду причин. Кроме того, как отметил ЕСПЧ в решении по делу Захарова, отсутствие требования уведомлять о слежке на деле зачастую подрывает эффективность средств правовой защиты от нарушений прав в связи с тайной слежкой.

Правительство Беларуси обращает внимание на то, что статьи 10 и 11 закона ОРД оставляют за гражданами право жалобы на меры наблюдения в соответствии с актами законодательства. Однако, как демонстрируется ниже, эти акты законодательства содержат спорные требования, например, касательно предварительного обжалования в органах, вышестоящих по отношению к тем, на которые направляется жалоба.

Глава 16 Уголовно-процессуального кодекса предусматривает право участников уголовного процесса на жалобы. Жалобы на действия прокурора или следователя направляются вышестоящему прокурору или следователю.[157]

Глава 29 Гражданского процессуального кодекса позволяет лицам жаловаться на действия государственных органов в случае нарушения своих прав. Жалоба подаётся в суд только после жалоб в вышестоящие органы по отношению к совершившим нарушение.[158]

Согласно статье 938 Гражданского кодекса граждане могут обратиться за возмещением ущерба за вред, причинённый государственными органами.[159]

На деле эти средства защиты оказываются неэффективными. Как отмечается ниже, многие активисты не слишком стремятся прибегать к средствам защиты, поскольку не верят в независимость и действенность судебной системы. Кроме того, требование жаловаться в вышестоящие органы подрывает эффективность средств защиты, поскольку, как отметил ЕСПЧ в решении по делу Захарова, **«обращение в порядке иерархии в орган, непосредственно вышестоящий над тем, чьи действия стали предметом жалобы, не отвечает стандартам независимости, необходимым для достаточной защиты от злоупотребления полномочиями».**[160] Далее ЕСПЧ отметил, что и в гражданских, и в уголовных делах, когда бремя доказывания возлагается на истца, «в отсутствие уведомления либо доступа к официальным документам в какой бы то ни было форме, относящимся к перехвату информации, выполнить требования такого бремени доказывания практически невозможно».[161]

Это повторили и активисты гражданского общества Беларуси, отмечая, что хотя опротестовать подозреваемую незаконную слежку теоретически можно, на деле это практически невозможно из-за малой вероятности представить весомые доказательства.[162] Один независимый журналист отметил: «Многих этих случаев мы просто не знаем. Доказательства всплывают только на суде».[163] Адвокат-правозащитник сказал, что ему неизвестно о каких-либо случаях, когда лица, пострадавшие в результате незаконной слежки, успешно воспользовались средствами правовой защиты».[164]

Отсутствие доверия к действенности имеющихся средств правовой защиты также лишает людей желания попытаться найти прямые доказательства возможной незаконной слежки. Политик-оппозиционер, также отметивший, что уверен, что его учётную запись взломал КГБ, сказал: «Какой смысл выяснять кто и что взламывает? Потому что в Беларуси с этим всё равно нельзя обратиться в суд. Так это что неважно. Важно как можно скорее восстановиться и продолжать работать».[165] Молодёжный активист отметил: «У меня такое впечатление, что за мной почти постоянно следят. Но опротестовывать слежку я бы никогда не стал. В конце концов это же меня арестовали по нелепым обвинениям только за то, что я был на улице. Если на всё жаловаться, то можно всю жизнь провести в суде безрезультатно».[166]

(a) обеспечить любому лицу, права и свободы которого, признаваемые в настоящем Пакте, нарушены, эффективное средство правовой защиты, даже если это нарушение было совершено лицами, действовавшими в официальном качестве;
(b) обеспечить, чтобы право на правовую защиту для любого лица, требующего такой защиты, устанавливалось компетентными судебными, административными или законодательными властями или любым другим компетентным органом, предусмотренным правовой системой государства, и развивать возможности судебной защиты;
(c) обеспечить применение компетентными властями средств правовой защиты, когда они предоставляются».

[157] Уголовно-процессуальный кодекс, глава 16, статья 139, http://kodeksy.by/ugolovno-processualnyy-kodeks/
[158] Гражданский процессуальный кодекс, глава 29, статья 354, http://kodeksy.by/grazhdanskiy-processualnyy-kodeks/VII-glava-29
[159] Гражданский кодекс Республики Беларусь, статья 938, http://xn----7sbakgchdukjdc8auvwj.xn--90ais/statya-938
[160] Дело Захарова, п. 292.
[161] Дело Захарова, п. 296.
[162] Беседа с правозащитником, Минск, декабрь 2015 года.
[163] Беседа с независимым журналистом, Минск, декабрь 2015 года.
[164] Беседа с правозащитником, Минск, декабрь 2015 года.
[165] Беседа с политическим оппозиционером, Варшава, август 2015 года.
[166] Удалённая беседа с молодёжным активистом, Лондон, март 2016 года.

«СУДЕБНАЯ СИСТЕМА ПО-ПРЕЖНЕМУ ПОЛНОСТЬЮ ЗАВИСИТ ОТ ПРЕЗИДЕНТА, НЕСМОТРЯ НА НЕДАВНИЕ РЕФОРМЫ. ПОМИМО ОТСУТСТВИЯ НЕЗАВИСИМОСТИ СУДОВ И ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ АДВОКАТОВ ЗАПУГИВАЮТ, ЗАСТАВЛЯЯ ИХ ВСТУПАТЬ В АДВОКАТСКИЕ КОЛЛЕГИИ, НЕПОСРЕДСТВЕННО ПОДКОНТРОЛЬНЫЕ ПРАВИТЕЛЬСТВУ».

Специальный докладчик ООН по вопросу о положении в области прав человека в Беларуси, апрель 2015 года[167]

Многие из тех, с кем беседовала Amnesty International, также ссылались на отсутствие веры в справедливость судебной системы как на сдерживающий фактор, не позволяющий им прибегать к средствам правовой защиты в случаях незаконной слежки. Как отмечается выше, закон предусматривает жалобы на ненадлежащие действия должностных лиц, по крайней мере в первую очередь, непосредственно в вышестоящие инстанции по отношению к тем, против которых направляется жалоба. Как отмечал Европейский суд по правам человека, при такой системе отсутствует независимость, достаточная для гарантии защиты от произвола.[168] Когда Amnesty International спросила одного активиста, почему тот не пытался возместить ущерб, причинённый в результате слежки, он пояснил: «Прежде всего, у меня нет доказательств в обоснование жалобы. Во-вторых, не думаю, что я вообще буду подавать какие-то жалобы. Я достаточно общался с нашей судебной системой и правоохранительными органами и знаю, как они работают. Кроме того, я вообще не сторонник жалоб “экзекутеру” на действия другого “экзекутора”».[169] Аналогично, другой активист на вопрос о том, пытался ли он возместить ущерб, причинённый слежкой, ответил: «Жаловаться на тех самых людей, которые меня преследовали? Единственный способ пожаловаться, о которым я бы подумал, это обращение в Европейский суд по правам человека. Но, как ни печально, нам этот способ недоступен, потому что Беларусь не входит в состав Совета Европы».[170] Журналистка, оказавшаяся в тюрьме отчасти на основании доказательств, полученных в результате слежки, которую она считала незаконной, сказала, что не думала о возмещении ущерба, поскольку просто больше не хотела иметь никаких дел с милицией.[171]

Как сказал один журналист, «Здесь свободных судов нет. Все судьи назначаются указом президента… Поэтому такой мера борьбы с действиями властей как обращение в суд здесь существует».[172]

Других беспокоило то, что их статус ставит их в неблагоприятное положение в плане возмещения ущерба. Один студент-активист отметил, что даже оппозиционным кандидатам на пост президента не удалось возместить ущерб от незаконной слежки, поэтому он сомневается, что это удастся студенту-активисту.[173] Политик-оппозиционер подчеркнул, что возмещение ущерба даже может обернуться угрозой активистам с правовой точки зрения. «Были способы подать заявления в некоторые органы. Например, можно было вернуться к ним в офис и пожаловаться, спросить, почему за мной следили, поскольку я знал, что мои переговоры прослушивались и что было услышано. Конечно, это возможно, но смысла в этом не было. Совершенно никакого смысла. Просто будет волокита. К тому же из-за характера нашей повседневной работы мы должны помнить, что против нас могут использовать статью 193-1 Уголовного кодекса. Это статья о деятельности общественных организаций. Согласно этой статье, нас в любую минуту могут арестовать, потому что наша организация не зарегистрирована».[174]

---

[167] Доклад Специального докладчика ООН по вопросу о положении в области прав человека в Беларуси Миклоша Харашти, A/HRC/29/43, (29 апреля 2015 г.).
[168] Дело Захарова, п. 292
[169] Беседа с молодёжным активистом, Минск, декабрь 2015 года.
[170] Удалённая беседа с молодёжным активистом, Лондон, апрель 2016 года.
[171] Беседа с независимой журналисткой, Минск, декабрь 2015 года.
[172] Беседа с независимым журналистом, Минск, декабрь 2015 года.
[173] Беседа со студентом-активистом, Минск, декабрь 2015 года.
[174] Беседа с активистом политической оппозиции, Минск, декабрь 2015 года. Деятельность незарегистрированных организаций запрещается Уголовным кодексом Республики Беларусь, см. выше «Ограничительная правовая база в отношении гражданского общества».

В некоторых случаях пострадавшие в результате возможных хакерских атак, например, Леонид Судаленко и Александр (см. выше), обращались в милицию не потому что считают, что это принесёт результат, а для того, чтобы защититься от уголовного преследования.

На этом фоне всеобщего скептицизма по поводу пользования средствами правовой защиты через судебную систему попытки оппозиционных политиков добиться расследования случая, когда в держателе для салфеток в кафе, где они встречались, по-видимому, обнаружилось подслушивающее устройство (см. выше), относительно редки. Их усилия результатов не принесли.

Пятнадцатого октября 2015 года политики направили заявление о возбуждении уголовного дела в Генеральную прокуратуру и потребовали предъявить им ордер на перехват их сообщений, а также подтвердить, продолжается ли за ними слежка. Несколько дней спустя они получили ответ из Центрального управления внутренних дел Минска, в котором просто говорилось, что по итогам проверки на основании их заявления в возбуждении уголовного дела отказано за отсутствием доказательств. По словам политиков, милиция не вызывала их для дачи показаний и не потребовала жучок на экспертизу. Политики решили не опротестовывать решение об отказе в возбуждении уголовного дела, поскольку считали, что это решение оставят в силе.[175]

[175] Беседа с Объединённой гражданской партией, Минск, декабрь 2015 года.

7 РОЛЬ ЧАСТНЫХ КОМПАНИЙ

Негласное наблюдение в Беларуси возможно благодаря тому, что государство получает прямой доступ как к сохранённым данным, так и к данным в режиме реального времени у операторов связи, работающих в Беларуси.

Как изложено в Руководящих принципах предпринимательской деятельности в аспекте прав человека ООН (РППД), компании обязаны соблюдать права человека, где бы в мире они ни работали. РППД требуют от компаний активно заботиться о том, чтобы не вызывать нарушений прав человека и не способствовать им в рамках своей глобальной деятельности и принимать ответные меры, если они происходят. Для выполнения этой обязанности компании должны обеспечивать должную заботу о правах человека «в целях выявления, предотвращения, смягчения последствий и представления отчётности о том, каким образом они устраняют оказываемое ими воздействие на права человека», а также последствия их деловых отношений либо действий их дочерних компаний в этой связи. Корпоративная ответственность в отношении прав человека существует независимо от способности или готовности государства соблюдать собственные обязательства в области прав человека сверх соблюдения национального законодательства и регламента, защищающего права человека. Это значит, что в случаях, когда белорусское законодательство не отвечает нормам и стандартам международного права в области прав человека, работающие в Беларуси компании всё равно должны обеспечивать соблюдение прав человека в ходе своей деятельности на территории Беларуси. Например, в РППД, в частности, отмечается, что компания способствует нарушению прав человека, если предоставляет «данные о пользователях интернет-сервисами правительству, которое использует эти данные с целью уголовного преследования и слежки за политическими диссидентами в нарушение прав человека».[176]

> «В СИТУАЦИЯХ, КОГДА КОМПАНИИ СТАЛКИВАЮТСЯ С ТРЕБОВАНИЯМИ ПРАВИТЕЛЬСТВА ОБЕСПЕЧИТЬ ДОСТУП К ИНФОРМАЦИИ, КОТОРАЯ НЕ СООТВЕТСТВУЕТ МЕЖДУНАРОДНЫМ ПРАВОЗАЩИТНЫМ СТАНДАРТАМ, ОНИ ДОЛЖНЫ СТРЕМИТЬСЯ КАК МОЖНО БОЛЕЕ ПОЛНО УВАЖАТЬ ПРИНЦИПЫ ЗАЩИТЫ ПРАВ ЧЕЛОВЕКА И БЫТЬ ГОТОВЫМ ПРОДЕМОНСТРИРОВАТЬ СВОИ ПОСТОЯННЫЕ УСИЛИЯ, ПРЕДПРИНИМАЕМЫЕ В ЭТОМ НАПРАВЛЕНИИ».
>
> Верховный комиссар Организации Объединенных Наций по правам человека[177]

Три крупнейших оператора мобильной связи в Беларуси — это МТС, Life:) и «Велком». Совместными владельцами МТС (Беларусь) являются российская компания МТС и «Белтелеком», государственный провайдер телекоммуникационных услуг и интернета. Владельцем компании Life:) на 80% является турецкая компаний Turkcell.[178] В свою очередь 38% её принадлежит шведской компании Teliasonera.[179] Владельцем «Велком» является дочерняя компания of Telekom Austria Group, которой в свою очередь более чем на 60% владеет América Móvil.[180]

[176] Руководящие принципы предпринимательской деятельности в аспекте прав человека, стр. 17 http://www.ohchr.org/Documents/Issues/Business/RtRInterpretativeGuide.pdf
[177] УВКПЧ ООН, Право на неприкосновенность личной жизни в цифровой век, п. 45.
[178] http://www.life.com.by/private/about/life/myi_-_chast_bolshoy_gruppyi
[179] http://www.teliacompany.com/en/about-the-company/markets-and-brands/turkey/
[180] http://www.telekomaustria.com/en/group/belarus; http://www.telekomaustria.com/en/ir/shareholder-structure

Amnesty International связалась с МТС (Беларусь), Life:), «Велком», «Белтелеком», Telekom Austria Group, Teliasonera и Turkcell, чтобы запросить информацию о принятых ими мерах по выявлению, предотвращению и смягчению последствий незаконной слежки за их абонентами в Беларуси и представления отчётности об этом.

Из компаний, ответивших на письма Amnesty International, Teliasonera отметила ряд мер, принятых в отношении своей деятельности и деятельности своих дочерних компаний в других странах. Компания заявила, что придерживается жёсткой политики, выступая против прямого доступа к телекоммуникациям и связанных с ними данных: «Мы выступаем за то, что у правительств не должно быть прямого доступа к сетям и системам компании. Компания должна сохранять за собой операционный и технический контроль». Teliasonera также публично выступала против требований прямого доступа.[181] Кроме того, компания обратила внимание на своё участие в инициативе «Отраслевой диалог в сфере телекоммуникаций» (Telecoms Industry Dialogue)[182] и отметила, что публикует отчёт о прозрачности[183], в который входит информация о числе запросов данных абонентов во многих странах, где работает Teliasonera, а что касается стран прямого доступа, где такую информацию получить невозможно, отчёт включает сведения о соответствующей правовой базе, а также о политике компании в области свободы выражения мнения.[184]

Эти шаги можно только приветствовать, однако они не имеют прямого отношения к Беларуси. Согласно позиции компании по этому вопросу, она не работает на территории Беларуси, поскольку не является мажоритарным владельцем Turkcell (компании, контролирующей Life:)) и не представлена в правлении Turkcell. В ответ на сообщения СМИ Teliasonera подтвердила, что два человека, номинированные ей в 2013 году в правление Turkcell, были приняты в состав правления, но при этом подчеркнула, что эти лица считают себя независимыми. Кроме того, Teliasonera заявила, что с тех пор ей не представлялась возможность номинировать членов правления. Вместе с тем компания заявила, что «обратила внимание Turkcell на значение свободы выражения мнения и неприкосновенности частной жизни, и мы также рассказали им о своей политике и о том, как мы работаем».[185] Что касается позиции Teliasonera, Amnesty International считает, что она расходится с обязательством компании проявлять должную заботу о правах человека, «которая может быть непосредственно связана с её деятельностью, продукцией или услугами через её деловые отношения».[186]

Telekom Austria Group (владелец «Велком») также ответила Amnesty International. На встрече, а также в последующей переписке с организацией компания заявила, что связана обязательством выполнять требования белорусского законодательства. Компания заявила, что предоставила информацию о международных стандартах белорусским властям и обратила их внимание на «проблематичность» некоторых действий правительства в отношении данных пользователей, но отказалась привести примеры. Telekom Austria Group не публикует доклады о прозрачности и никакую другую информацию о правовой базе или практике, регулирующей доступ к данным абонентов «Велком»в Беларуси.[187] Соответственно, Telekom Austria Group, по всей видимости, не выполняет своих обязательств по части должной заботы в вопросах прав человека, возникающих в ходе деятельности своей дочерней белорусской компании «Велком».

Другие телекоммуникационные компании, которым писала Amnesty International, то есть «Велком», Life:), МТС (Беларусь), «Белтелеком» и Turkcell, на наши письма не ответили. В результате исследований нам не удалось обнаружить в свободном доступе информацию, которая указывала бы на то, что эти компании предпринимали шаги, направленные на выявление, предотвращение, смягчение последствий и представление отчётности о том, каким образом они устраняют оказываемое ими воздействие на права человека. Соответственно, при отсутствии доказательств обратного, они, по всей видимости, также не выполняют обязательства по части должной заботы относительно этих проблем прав человека.

---

[181] См. Freedom Online Coalition, WG2: Rule of Law Blog Series, Blog #2: Direct Access Systems and the Right to Privacy («Рабочая группа-2, Серия блогов о верховенстве закона, блог №2: Системы прямого доступа и право на неприкосновенность частной жизни», на англ. яз.) https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-group-2/direct-access-systems/

[182] http://www.telecomindustrydialogue.org/

[183] http://www.teliacompany.com/en/sustainability/reporting/law-enforcement-disclosure-report/

[184] http://www.teliacompany.com/globalassets/telia-company/documents/about-teliasonera/public-policy/teliasonera_group-policy_freedom-of-expression-in-telecommunications.pdf

[185] Электронная переписка от 25 мая 2016 года (хранится у Amnesty International). Turkcell не ответила на просьбу Amnesty International предоставить информацию.

[186] ООН, Руководящие принципы предпринимательской деятельности в аспекте прав человека, принцип 17(a), http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_RU.pdf

[187] Телеконференция с представителями Telekom Austria Group, 9 июня 2016 года. Компания «Велком» не ответила на просьбы Amnesty International предоставить информацию.

8 ЗАКЛЮЧЕНИЕ

Белорусское законодательство позволяет властям прибегать к масштабной слежке практически по любой причине и не требует независимой судебной санкции или надзора. Посредством системы СОРМ власти получают прямой, непрерывный, удалённо контролируемый доступ к коммуникациям и связанным с ними данным. Мобильные операторы и интернет-провайдеры, а также другие компании связи содействуют этому спорному прямому доступу властей к данным своих абонентов. Из-за полной секретности, окружающей практику слежки, о ней практически невозможно узнать, не говоря о том, чтобы опротестовать незаконную практику наблюдений. Эта система далеко не отвечает требованиям норм и стандартов международного права, применимым к наблюдению как к законному средству правоохранительной деятельности.

Использование личных данных и коммуникаций с целью уголовного преследования людей после выборов 2010 года дало понять многим белорусам: они должны считать, что им постоянно грозит слежка.

Это вредит гражданскому обществу Беларуси, которое и без того жёстко связано ограничительной правовой базой, регулирующей прочие аспекты их работы в стране. Поскольку такие законные действия, как действие от имени незарегистрированной организации или участие в мирном протесте могут повлечь уголовное преследование, многие активисты прибегают к самоцензуре и воздерживаются от реализации своих прав. Их законная работа в итоге становится всё труднее, поскольку такие простые задачи, как поиски финансирования для своей организации, телефонные звонки или организация встреч несут с собой риск — реальный или мнимый.

Хотя криптографическая защита и другие средства сохранения конфиденциальности могут помочь защитить некоторые личные данные, они не могут устранить риск слежки, с которым сталкиваются активисты. Мобильные телефоны всё также могут использоваться для прослушивания частных переговоров и определения местонахождения. Компьютеры и телефоны всё так же подвержены взломам, власти обладают полномочиями изымать устройства, а это приводит к тому, что активисты в дальнейшем боятся ими пользоваться.

Возникающий в итоге сковывающий эффект приводит к сужению пространства для гражданского общества и отрицательно воздействует на права человека в Беларуси, в том числе на право на информацию, поскольку всё меньше активистов, независимых журналистов и других могут представлять мнения, противоречащие официальным.

Сковывающий эффект, возникающий в результате слежки — не случайность. Сравнение слежки в Беларуси с нормами и стандартами международного права, особенно с решением Европейского суда по правам человека по делу Захарова, подчёркивает, что этот сковывающий эффект стал прямым результатом законов и практики, регулирующих слежку. Это вызывает нарушения прав на неприкосновенность частной жизни, свободу выражения мнения, свободу мирных собраний и объединений и других прав. Правительство нарушает эти права не только непосредственно следя за активистами по причине их законной деятельности, но также сохраняя законы и практики, относящиеся к слежке, которые заставляют людей прибегать к самоцензуре.

9 РЕКОМЕНДАЦИИ

9.1 ИСПОЛНИТЕЛЬНОЙ И ЗАКОНОДАТЕЛЬНОЙ ВЕТВЯМ ПРАВИТЕЛЬСТВА РЕСПУБЛИКИ БЕЛАРУСЬ

1. Реформировать законодательство, относящееся к слежке, в том числе закон «Об оперативно-розыскной деятельности» (№ 307-З от 15 июля 2015 года) и Уголовный кодекс, приведя правовой режим и относящуюся к нему практику в соответствие с нормами и стандартами международного права в области прав человека.
2. Обеспечить, чтобы общественности была доступна информация, относящаяся к законам и практике касательно слежки как минимум в той мере, которая предусмотрена Глобальными принципами национальной безопасности и правом на информацию (принципами Тсване).
3. Помимо прочего следует принять меры, нацеленные на обеспечение следующего:

    - государственные органы должны предъявлять утверждённые судом запросы о предоставлении им телекоммуникационных данных, а не пользоваться прямым, удалённо контролируемым доступом;
    - от поставщиков телекоммуникационных услуг не следует требовать сохранять данные коммуникаций вне условий уголовного расследования, а лишь на основании судебного ордера, содержащего надлежащую информацию о конкретном лице и разумные подозрения в совершении противоправных действий;
    - перехват сообщений и доступ к связанным с ними данным допускается только при наличии санкции, выданной или соответственно продлённой независимым судебным органом, который должен оценить наличие конкретных разумных подозрений в совершении противоправных действий лицом, подвергающимся слежке; судебный орган должен быть удовлетворён, что при этом соблюдены критерии необходимости и соразмерности;
    - правовые основания тайного наблюдения, в том числе определение национальной безопасности, надлежит включить в законодательство и определить их столь подробно и узко, чтобы они отвечали стандарту ясности и точности и были бы достаточны для разъяснения лицам обстоятельств, которые могут привести к слежке;
    - полномочия по проведению тайного наблюдения должны подлежать надзору со стороны действительно независимого надзорного органа, обладающего достаточной материальной базой, прозрачного для общественности, имеющего доступ ко всей информации и обладающего полномочиями и мандатом выявлять, расследовать и прекращать тайную слежку, а также предоставлять средства правовой защиты в случаях связанных с ней нарушений прав человека;
    - внести поправки в законодательство, чётко ограничив продолжительность тайного наблюдения во всех случаях;
    - законодательно предусмотреть требования об уничтожении всех связанных со слежкой данных;
    - лиц, подвергающихся слежке, следует уведомлять о том, что за ними следили, если это не противоречит или более не противоречит законной цели текущего расследования;
    - обеспечить доступ к средствам эффективной правовой защиты и позволить гражданам опротестовывать меры наблюдения либо нарушения своих прав в связи со слежкой в независимом суде со всеми необходимыми гарантиями надлежащего процесса;
    - предать огласке достаточную информацию о технических данных систем слежки, включая средства взлома.

9.2 ПРОКУРОРАМ

Пока полномочия касательно санкционирования тайного наблюдения не переданы независимому судье, прокуроры должны:

1. позаботиться о том, чтобы запросы о тайной слежке санкционировались только на основании подробных и конкретных разумных подозрений в совершении противоправных действий объектом слежки и при условии, что эти запросы отвечают критериям необходимости и соразмерности;

2. регулярно публиковать отчёты, как минимум содержащие информацию о числе представленных запросов о слежке — как утверждённых, так и отклонённых, с разбивкой по направляющему их органу и правовым основаниям;

3. обеспечить, чтобы санкция не выдавалась на основании пользования правами человека, включая участие в незарегистрированных организациях и в мирных собраниях;

4. пользоваться полномочиями надзора за применением мер наблюдения, а при наличии доказательств нарушения закона или прав человека обеспечивать их прекращение и привлекать виновников к ответственности.

9.3 ОРГАНАМ, ОСУЩЕСТВЛЯЮЩИМ ОПЕРАТИВНО-РОЗЫСКНУЮ ДЕЯТЕЛЬНОСТЬ

До принятия рекомендованных выше реформ:

1. регулярно публиковать отчёты, как минимум включающие информацию о числе запросов о проведении тайной слежки — утверждённых или отклонённых, с разбивкой по правовым основаниям;

2. публиковать информацию о том, сколько раз использовалась система СОРМ для доступа к данным, а также о правовых основаниях её использования;

3. воздерживаться от запросов о слежке на основании пользования правами человека, включая участие в незарегистрированной организации или в каких-либо мирных собраниях.

9.4 ТЕЛЕКОММУНИКАЦИОННЫМ КОМПАНИЯМ

1. Обеспечить должную заботу о правах человека в целях выявления, предотвращения, смягчения последствий и представления отчётности о том, каким образом устраняется оказываемое ими и их дочерними компаниями воздействие на права человека в Беларуси и других странах, включая как минимум:

- опротестование законодательных требований, противоречащих нормам и стандартам международного права в области прав человека;
- регулярные публикации данных о числе запросов о доступе к данным сообщений абонентов и связанных с ними данных и о случаях такого доступа; по возможности публиковать подробную и доступную информацию относительно законодательной базы и практики, регулирующей раскрытие данных абонентов государственным органам;
- добиваться переговоров о пересмотре требований касательно использования системы СОРМ, а также о пересмотре правовых и других обязательств, касающихся раскрытия данных абонентов, не отвечающих нормам и стандартам международного права.

AMNESTY INTERNATIONAL —
ВСЕМИРНОЕ ДВИЖЕНИЕ
ЗА ПРАВА ЧЕЛОВЕКА.
КОГДА С КЕМ-ТО ПОСТУПАЮТ
НЕСПРАВЕДЛИВО,
ЭТО ВАЖНО ДЛЯ ВСЕХ НАС.

СВЯЗАТЬСЯ С НАМИ

INFO@AMNESTY.ORG

+44 (0)20 7413 5500

УЧАСТВУЙТЕ В ОБСУЖДЕНИИ

WWW.FACEBOOK.COM/AI RUSSIA

@AMNESTY

AMNESTY INTERNATIONAL

« ДОСТАТОЧНО ОСОЗНАВАТЬ, ЧТО ОНА ЕСТЬ»

Гражданское общество, секретность и слежка в Беларуси

Белорусское законодательство позволяет властям прибегать к масштабной слежке практически по любой причине без независимого контроля. Система тайного наблюдения вредит гражданскому обществу в Беларуси, деятельность которого и без того серьёзно подрывается угрозой уголовного или административного наказания лишь за осуществление прав человека, например, за участие в протестах.

В подобной обстановке страх перед слежкой оказывает сковывающий эффект, из-за которого даже такие простые повседневные дела, как телефонный звонок, организация встреч и планирование общественных мероприятий, становятся труднее и опаснее. Мобильные телефоны могут использоваться для прослушивания частных переговоров, отслеживания местонахождения и выяснения, с кем встречался его владелец. Личная информация из электронных писем или записей в социальных сетях может грозить активистам привлечением к уголовной ответственности, если их переписку взломают.

Белорусская система практически не предусматривает средств правовой защиты для лиц, чьи права оказались нарушены в результате слежки. Существованию этой системы способствует сотрудничество с властями белорусских и иностранных телекоммуникационных компаний, предоставляющих им прямой доступ к данным абонентов через систему СОРМ.

В настоящем докладе предлагаются рекомендации белорусскому правительству, а также белорусским и иностранным телекоммуникационным компаниям о мерах по прекращению связанных со слежкой нарушений прав человека в Беларуси.