Global Freedom of Expression
COLUMBIA UNIVERSITY

Манохар (Manohar) против Индийского союза

Индия, Азия и Азиатско-тихоокеанский регион

Завершено
Расширяет сферу защиты права

ФОРМА ВЫРАЖЕНИЯ
Электронное/интернет-сообщение, пресса/газеты

ДАТА ПРИНЯТИЯ РЕШЕНИЯ
27 октября 2021 г.

НОМЕР ДЕЛА
ходатайство о вынесении судебного приказа (в уголовном деле) № 314 от 2021 г.

СУДЕБНЫЙ ОРГАН
Верховный суд (суд последней инстанции)

ОБЛАСТЬ ПРАВА
Конституционное право

ОСНОВНЫЕ ТЕМЫ
Свобода прессы, национальная безопасность, неприкосновенность частной жизни, защита и хранение данных

ИТОГИ
Ходатайство удовлетворено

ТЭГИ
Национальная безопасность, неприкосновенность частной жизни, свобода прессы, слежка

Обзор включает в себя:

- **Анализ дела**
- **Ориентация решения**
- **Перспектива**
- **Значение**

АНАЛИЗ ДЕЛА

Резюме и итоги

Верховный суд Индии признал наличие достаточных оснований для создания экспертной комиссии по изучению обвинений в несанкционированной слежке и нарушении неприкосновенности частной жизни индийских граждан со стороны индийского правительства и иностранными организациями. Согласно результатам расследования, проведенного 17 медийными организациями со всего мира, многочисленные заявители, включая журналистов, адвокатов и других правозащитников, утверждали, что их цифровые устройства были взломаны шпионской программой Pegasus, разработанной израильской технологической фирмой. Суд постановил, что несанкционированная слежка за сохраненными данными с цифровых устройств граждан с помощью шпионских программ по причинам, не связанным с безопасностью страны, является незаконной, предосудительной и может иметь далеко идущие последствия не только для прав на неприкосновенность частной жизни, но и для прав на свободу выражения мнения. Суд счел, что отказ правительства предоставить информацию под предлогом обеспечения «национальной безопасности» не был достаточно обоснованным, и постановил создать независимую экспертную комиссию для расследования утверждений заявителей.

Факты

С иском по данному делу в суд обратилась группа индийских граждан, включая журналистов, адвокатов и правозащитников, утверждавших, что они напрямую пострадали от шпионского ПО «Pegasus», а также множество других лиц, отстаивающих общественные интересы и обеспокоенных несанкционированной слежкой и перехватом сообщений в Индии.

В сентябре 2018 года канадская исследовательская лаборатория Citizen Lab сообщила об использовании некоторыми неназванными государственными разведывательными и правоохранительными органами «пакета шпионских программ» «Pegasus», разработанного израильской технологической компанией (NSO Group). Это ПО взламывает цифровые устройства, обеспечивая доступ ко всем сохраненным в устройстве

данным, электронной почте, текстам, телефонным звонкам, камере и звукозаписям в режиме реального времени. Весь контроль над устройством передается пользователю ПО, который затем может удаленно управлять различными функциями устройства без каких-либо действий со стороны его владельца. По оценкам Citizen Lab, данная проблема затронула граждан почти 45 стран. В мае 2019 года компания WhatsApp Inc, специализирующаяся на обмене мгновенными сообщениями, объявила, что ПО «Pegasus» могло проникнуть на устройства пользователей WhatsApp. 20 ноября 2019 года тогдашний Почетный министр коммуникаций, информационных технологий, закона и правосудия Индии заявил в парламенте, что некоторые индийские граждане пострадали от этого программного обеспечения.

15 июня 2020 года Citizen Lab и Amnesty International объявили о разоблачении еще одной шпионской кампании, жертвами которой стали девять человек в Индии. 18 июля 2021 года 17 медийных организаций со всего мира, включая индийскую «The Wire», обнародовали список из примерно 50 000 мобильных номеров телефонов, в которые якобы проникло программное обеспечение «Pegasus» (а, следовательно, за ними следили клиенты NSO Group). В связи с этим ряд иностранных правительств начали взаимодействие с израильским правительством, в другие инициировали внутренние расследования этих заявлений. Утверждается, что около 300 из этих телефонных номеров принадлежали индийским журналистам, врачам, политическим деятелям и сотрудникам суда. На момент подачи письменных ходатайств было подтверждено, что указанное программное обеспечение было обнаружено на телефонах десяти индийских граждан.

18 июля 2021 года министр железных дорог, связи, электроники и информационных технологий (представляющий правительство Индии, которое является ответчиком в данном деле) поставил под сомнение фактическую основу этих заявлений и опроверг факт незаконного наблюдения. Министр также подчеркнул «чрезвычайно строгий» характер индийских законов, касающихся наблюдения, и заявил о невозможности осуществления незаконного наблюдения при таком режиме [п. 8].

10 августа 2021 года ходатайства были вручены Генеральному солиситору Индии. Заявители подали в Верховный суд Индии письменные иски в отношении ответчика (индийского правительства), требуя проведения независимого расследования обвинений в незаконном наблюдении, кибератаке и нарушении неприкосновенности их частной

жизни. Ссылаясь на непринятие ответчиком мер по надлежащему рассмотрению обвинений, выдвинутых в многочисленных сообщениях об использовании программного обеспечения «Pegasus», заявители выразили подозрение, что ответчик и его ведомства сами являлись клиентами «NSO Group» в нарушение установленных законодательством Индии требований в отношении проведения наблюдения.

Обзор решения

Председатель Верховного суда Индии Н. В. Рамана, судья Хима Кохли и судья Сурья Кант огласили решение Верховного суда Индии в составе коллегии из трех судей 27 октября 2021 года. Основным для рассмотрения был вопрос о наличии достаточных доказательств для возбуждения дела против ответчика в связи с предполагаемым несанкционированным наблюдением и нарушением неприкосновенности частной жизни, что дало бы основание для создания независимой комиссии для расследования этих обвинений.

Аргументы истцов:

Заявители выдвинули против ответчика различные аргументы, подкрепляя их показаниями экспертов по кибербезопасности, перепроверенными при помощи информации, полученной от различных авторитетных новостных организаций по всему миру, а также от таких организаций, как «Citizen Lab».

Наиболее важным представляется заявление истцов о том, что несанкционированная слежка, осуществляемая ответчиком с помощью шпионского ПО «Pegasus», не только нарушает их право на неприкосновенность частной жизни, но и оказывает «сдерживающее» воздействие на реализацию их свободы слова [п. 21].

Заявители утверждали, что данное ПО может использоваться не только для отслеживания мобильного устройства, но и с целью подбрасывания в него фальшивых документов и улик, которые могут послужить доказательством вины его владельца. Таким образом, ответчик обязан «принять необходимые меры для защиты интересов и фундаментальных

прав граждан, особенно в условиях существования риска совершения такой атаки иностранной организацией» [п. 19]. Аналогичным образом, заявители выразили «серьезную озабоченность» тем, что за признанием парламентом в 2019 году факта взлома в той или иной форме не последовало никаких последующих действий [п. 18]. Вместо этого, ответчик отказался предоставить им какую-
либо информацию по данному вопросу – и это сокрытие информации нарушает их основные права как граждан Индии.

Также было отмечено, что ответчик не сделал никакого конкретного заявления, опровергающего утверждения об использовании им программного обеспечения или иного способа незаконного наблюдения, что дает основания заключить, что ответчик признал эти обвинения. Кроме того, учитывая отсутствие опровержения, ответчику нельзя было доверить создание собственной комиссии для расследования данного дела – скорее, Суду следовало самому создать независимую комиссию во главе с отставным судьей, чтобы избежать любых «проблем с доверием», когда ни общественность, ни заявители не доверяли бы результатам расследования [п. 20].

Аргументы ответчика:

Ответчик представил «ограниченные письменные показания», утверждая, что запрашиваемая истцами информация о наблюдении не может быть обнародована, поскольку она может поставить под угрозу национальную безопасность Индии и может быть использована террористическими группами. Повторив заявление министра информационных технологий, ответчик подчеркнул, что не занимался незаконным наблюдением.

Ответчик был готов создать экспертную комиссию для расследования «всех аспектов» выдвинутых обвинений, а также для того, чтобы «развеять опасения общественности и устранить любые неверные представления» [п. 17]. Несмотря на опасения истцов, они утверждали, что у общественности нет причин сомневаться в надежности любого такой комиссии, созданной ответчиком.

Применимые правовые нормы

Как постановил Суд в знаковом деле 2017 года «К.С. Путтасвами (K. S. Puttaswamy) против Индийского союза», 10 SCC, право на неприкосновенность частной жизни в Индии является «таким же священным, как человеческое существование, и неотъемлемым для человеческого достоинства и автономии» [п. 32]. В этом деле суд признал, что право на неприкосновенность частной жизни не является абсолютным, и отметил конкурирующие права других конституционно обоснованных ограничений, в частности, таких как закон, оправдывающий вмешательство в частную жизнь при определенных обстоятельствах; требование о «законной цели государства», обеспечивающее, чтобы «характер и содержание вводящего ограничение закона находились в пределах разумного»; и соразмерность законодательства «объекту и потребностям, которые призван удовлетворить закон» [п. 34].

Право на неприкосновенность частной жизни в информационную эпоху

Как и в предыдущем решении по делу Путтасвами, Суд прежде всего подтвердил, что право на неприкосновенность частной жизни является «священным» и охраняется Конституцией [п. 32]. Суд отметил, что в эпоху «информационной революции, когда вся жизнь человека хранится в «облаке» или в цифровом досье», он вынужден признать способность технологий нарушать неприкосновенность частной жизни человека в той же мере, в какой они могут улучшить его жизнь [п. 31]. Кроме того, суд отметил, что информация о гражданах Индии в настоящее время собирается не только официальными государственными и разведывательными органами, но и финансовыми компаниями, при помощи телефонов, электронной почты и т.п., и может быть использована в законных целях, таких как предотвращение насилия и терроризма. Однако любой случай использования такой информации должен быть «основан на доказательствах», а также быть «абсолютной необходим для обеспечения национальной безопасности/интересов и... соразмерен» [п.п. 35-36]. Опираясь на статью 21 Конституции, Суд указал, что все граждане Индии как «члены цивилизованного демократического общества имеют разумные основания ожидать неприкосновенности своей частной жизни... [именно такое ожидание позволяет нам осуществлять наш выбор, права и свободы» [п. 32]. Однако, как указано выше, право на неприкосновенность частной жизни имеет разумные ограничения

– как и все другие основные права – и Суду необходимо будет соответствующим образом сбалансировать конкурирующие интересы.

Применяя эти правовые принципы к данному делу, Суд признал, что «в демократической стране, где царит верховенство закона, неизбирательная слежка за отдельными лицами допустима только при наличии достаточных правовых гарантий, с соблюдением процедуры, установленной законом в соответствии с Конституцией» [п. 36]. Суд постановил, что право на неприкосновенность частной жизни напрямую нарушается всякий раз, когда государство или любое внешнее ведомство наблюдает или шпионит за человеком, и что этот компромисс должен быть надлежащим образом уравновешен.

Слежка и свобода прессы

Далее Суд отметил, что угроза слежки или, более того, понимание, что за человеком могут следить, может сильно повлиять на то, каким образом он «решает реализовать свои права», и привести к самоцензуре, что особенно важно, когда речь идет о свободе прессы [п. 39]. Суд заявил, что «такое сдерживающее воздействие на осуществление свободы слова является посягательством на жизненно важную роль прессы как общественного наблюдателя, что может подорвать способность прессы предоставлять точную и достоверную информацию» [п. 39]. Ссылаясь на дело «Анурадха Бхасин (Anuradha Bhasin) против Индийского Союза», (2020) 3 SCC 637, Суд использовал критерий сравнительного вреда для оценки того, оказали ли установленные государством ограничения сдерживающее воздействие на других лиц в схожих обстоятельствах в течение того же периода времени, а также на любого другого истца, заявив, что без этих доказательств невозможно «отличить законное утверждение о сдерживающем воздействии от простого эмоционального довода, приведенного в корыстных целях» [п. 39].

Аналогичным образом, Суд подчеркнул важность защиты источников информации, как одного из важнейших условий свободы прессы в Индии. Без такой защиты источники могут быть лишены возможности оказывать содействие СМИ в информировании общественности по вопросам, представляющим жизненно важный общественный интерес [п. 40]. В связи с этим Суд постановил, что данное дело имеет «огромное значение», учитывая «важность защиты журналистских источников для свободы прессы

в демократическом обществе и потенциальный сдерживающий эффект, который могут оказать методы шпионажа» [п. 41].

Использование аргумента о «национальной безопасности»

Ответчик отказался предоставить суду достаточную информацию по данному вопросу, сославшись на интересы «национальной безопасности», и не разъяснил свою позицию по этим обвинениям или любым другим фактам по делу [п. 45]. Опираясь на прецедент, созданный в деле 2011 года «Рам Джетмалани (Ram Jethmalani) против Индийского Союза», 8 SCC 1, Суд осудил сокрытие ответчиком информации и применение иных способов, направленных на то, чтобы «держать истца в неведении», особенно в таком деле, как это, где речь идет об основных правах граждан, защищенных Конституцией [п. 46]. Примечательно, что Суд отметил, что предоставление информации ответчиком является «важным шагом на пути к прозрачности и открытости деятельности правительства, которые являются признанными ценностями согласно [Конституции]» [п. 47]. Хотя могут существовать особые обстоятельства, при которых ответчик может справедливо отстаивать свою позицию, отказывая Суду и/или истцам в доступе к определенной информации (например, с целью защиты суверенитета Индии, общественного порядка, в случае выражения неуважения к суду и т.п.), ответчик не может получать «поблажки» при каждом упоминании национальной безопасности, что превратило бы Суд в «немого наблюдателя», равно как и национальная безопасность не может быть «пугалом, одного лишь упоминания которого избегает судебная власть» [п.п. 49-50]. Суд постановил, что ответчик должен быть в состоянии четко обосновать, доказать и аргументировать, что в случае дачи им показаний может возникнуть конкретная конституционная проблема, или привести иные законные доводы в пользу своего освобождения от дачи показаний, наряду с соответствующими фактами, свидетельствующими о том, что сохранение указанной им информации в тайне действительно соответствует интересам национальной безопасности.

В данном случае ответчик не смог продемонстрировать, как раскрытие информации может повлиять на национальную безопасность, а простое упоминание национальной безопасности не препятствует осуществлению судом своих полномочий. Таким образом, суд пришел к выводу о наличии достаточных оснований для расследования заявлений, выдвинутых истцами.

Суд пришел к выводу, что существует «широкий консенсус в отношении того, что несанкционированная слежка/доступ к сохраненным данным с телефонов и других устройств граждан по причинам, не связанным с безопасностью страны, являются незаконными, предосудительными и вызывают обеспокоенность» [п. 52]. Исходя из этого, оставался вопрос о том, какое средство правовой защиты следует применить.

Независимая экспертная комиссия

Учитывая тот факт, что ответчик неоднократно уклонялся от дачи письменных показаний под присягой с изложением каких-либо фактов по делу или в связи с защитой национальной безопасности, Суд не пожелал обязывать ответчика к даче таких показаний с изложением соответствующих фактов. Вместо этого Суд принял решение о создании независимой экспертной комиссии под руководством отставного судьи Верховного суда Р. В. Равиндрана, который должен был изучить характер обвинений, «общественную значимость, а также предполагаемый масштаб и характер массового нарушения основных прав граждан страны» [п. 55]. В состав Комиссии вошла группа беспристрастных и независимых экспертов, состоявшая из бывшего офицера полиции Алока Джоши; председателя ISO/IEC д-ра Сундипа Обероя; профессора в области кибербезопасности и цифровой криминалистики д-р Навина Кумар Чаудхари; профессора инженерной школы д-ра П. Прабахарана и доцента кафедры д-ра Ашвина Анила Гумасте.

Суд обосновал необходимость создания комиссии рядом причин, включая возможное воздействие на право на частную жизнь и свободу слова, потенциальное «сдерживающее воздействие» этого дела на реализацию прав всего населения Индии, бездействие ответчика, тот факт, что правительство предположительно сознательно лишало своих граждан их прав, а также серьезность любого возможного участия иностранных лиц/государств, агентств или иных частных организаций [п. 56]. Суд отклонил предложение о том, чтобы сам ответчик назначил экспертную комиссию с целью расследования обвинений, поскольку такой порядок действий нарушил бы устоявшееся судебное правило против предвзятости, т.е. необходимость того, чтобы «правосудие должно не просто вершиться, но должно быть видно, что оно вершится» [п. 57].

Суд обратился к экспертной комиссии с просьбой проверить достоверность целого ряда фактов, включая то, использовалась ли шпионская программа «Pegasus» для получения доступа или иного способа перехвата информации, хранящейся в мобильных устройствах граждан Индии, какие граждане пострадали, была ли эта шпионская программа приобретена ответчиком, и если она использовалась, то на основании какого закона. Экспертную комиссию также попросили дать рекомендации по нескольким вопросам, включая необходимость принятия или изменения любых законодательных актов, касающихся наблюдения, повышения кибербезопасности, предотвращения вторжения в право граждан на частную жизнь с помощью шпионского ПО, создания механизма рассмотрения жалоб и независимого агентства для изучения вопросов уязвимости для кибератак [п. 61].

Заключение

Суд счел, что любые заявления о несанкционированном наблюдении или ином доступе к данным, хранящимся в устройствах граждан, в целях, выходящих за рамки национальной безопасности, являются «незаконными, вызывающими возражения и вызывающими беспокойство» [п. 52]. Учитывая потенциальные последствия для свободы прессы и права на неприкосновенность частной жизни, а также сокрытие ответчиком информации под предлогом обеспечения «национальной безопасности», Суд постановил создать независимую экспертную комиссию. Ответчику и связанным с ним агентствам/органам власти было предписано в случае необходимости оказывать комиссии полную поддержку. Суд потребовал, чтобы расследование и последующий отчет комиссии были подготовлены как можно скорее.

ОРИЕНТАЦИЯ РЕШЕНИЯ

Итог: **Решение суда расширяет сферу защиты права**

Верховный суд Индии расширил право на свободу выражения мнения в соответствии с Конституцией, увязав его по значению с правом на неприкосновенность частной жизни всех своих граждан, включая журналистов. Постановив, что несанкционированное наблюдение и угроза слежки могут не только привести к самоцензуре, но и поставить под

угрозу безопасность журналистских источников и надлежащее функционирование средств массовой информации в условиях демократии, Суд в решительно защитил право на свободу выражения мнения, увязав его с более широким понятием достойной и цивилизованной жизни граждан Индии.

ПЕРСПЕКТИВА

Перечень справочных документов

В списке источников на английском языке указаны документы, не имеющие официального перевода на русский язык.

Национальные стандарты, законодательство или судебная практика

- India, Keshavanand Bharti v. State of Kerala (1973) 4 SCC 225
- India, Justice Puttaswamy (Retd) & Anr v. Union of India & Ors (2017), 10 SCC 1
- India, Bhasin v. Union of India (2020), Writ Petition (Civil) No. 1031/2019.
- India, Indian Express Newspapers (Bombay) Private Ltd. v. Union of India, (1985) 2 S.C.R. 287
- India, Ram Jethmalani & Ors. v. Union of India, (2011) 8 SCC 1

ЗНАЧЕНИЕ

Решение создает обязательный или убедительный прецедент в рамках своей юрисдикции.

Ссылки на решение по данному делу содержатся в следующих делах:

- **««Форум по правам нубийцев» против генерального прокурора»**

ОФИЦИАЛЬНЫЕ ДОКУМЕНТЫ ПО ДЕЛУ

- Судебное решение (на английском языке)

Сообщения, аналитические и новостные статьи:

- **[Pegasus]"We Don't Want A Government That Might Have Used Pegasus to Set Up a Committee Of Its Own": Kapil Sibal Submits Before Supreme Court https://www.livelaw.in/top-stories/pegasus-supreme-court-government-committee-kapil-sibal-it-act-infiltration-179670**
- **Pegasus- Supreme Court Hearing-Oral Arguments https://www.livelaw.in/top-stories/pegasus-snoop-gate-supreme-court-sit-probe-181466?infinitescroll=1**
- **How do we read the Supreme Court's Pegasus order https://indianexpress.com/article/opinion/columns/pushback-on-pegasus-supreme-court-7594173/**
- **The Court's order on Pegasus still falls short https://www.thehindu.com/opinion/lead/the-courts-order-on-pegasus-still-falls-short/article37274506.ece**
- **Indian supreme court orders inquiry into state's use of Pegasus spyware https://www.theguardian.com/news/2021/oct/27/indian-supreme-court-orders-inquiry-into-states-use-of-pegasus-spyware**
- **A credible probe: On Supreme Court verdict on Pegasus row https://www.thehindu.com/opinion/editorial/a-credible-probe-the-hindu-editorial-on-supreme-court-verdict-on-pegasus-row/article37200571.ece**
- **The spyware is sold to governments to fight terrorism. In India, it was used to hack journalists and others. https://www.washingtonpost.com/world/2021/07/19/india-nso-pegasus/**