«Privacy International», «La Quadrature du Net» и др

Соединенное Королевство, Европа и Центральная Азия

Завершено
Расширяет сферу защиты права

ФОРМА ВЫРАЖЕНИЯ
Электронное/интернет-сообщение

ДАТА ПРИНЯТИЯ РЕШЕНИЯ
6 октября 2020 г

НОМЕР ДЕЛА
дело C-623/17, дела C-511/18, C-512/18, C-520/18

СУДЕБНЫЙ ОРГАН
Суд Европейского Союза

ОБЛАСТЬ ПРАВА
Гражданское право, конституционное право

ОСНОВНЫЕ ТЕМЫ
Конфиденциальность/неприкосновенность частной жизни, защита и хранение данных

ИТОГИ
Отмена или признание закона или иска неконституционными, консультативное заключение /предварительное решение

ТЭГИ
Защита и хранение данных, право на неприкосновенность частной жизни

Обзор включает в себя:

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

АНАЛИЗ ДЕЛА

Резюме и итоги

Большая палата Суда Европейского Союза (далее «Суд ЕС») в двух взаимосвязанных решениях установила, что законодательство ЕС ограничивает действие национального законодательства, обязывающего поставщиков услуг электронной связи осуществлять общую и неизбирательную передачу данных о трафике и местоположении пользователей службам безопасности и разведки в целях обеспечения национальной безопасности. В ходе рассмотрения объединенных заявлений Великобритании, Франции и Бельгии Суд ЕС попытался определить законность национального законодательства, обязывающего поставщиков услуг электронной связи передавать данные о трафике и местоположении пользователей государственным органам или сохранять такие данные в общем или неизбирательном порядке в целях предотвращения преступлений и обеспечения национальной безопасности. Суд установил, что такое обязательство не только препятствует защите права на неприкосновенность частной жизни и конфиденциальность персональных данных, но и противоречит принципу свободы выражения мнения в соответствии со статьей 11 Устава ЕС. При этом Суд указал, что в случаях, когда сохранение данных оправдано наличием серьезной угрозы национальной или общественной безопасности, характер такой меры должен быть «строго» соразмерен ее цели. Кроме того, Суд уточнил объем полномочий, предоставленных государствам-членам Директивой о конфиденциальности и электронных средствах связи в отношении сохранения данных для вышеупомянутых целей.

Факты

Хранение персональных данных в секторе электронных средств связи и получение доступа к этим данным в целях обеспечения национальной безопасности и борьбы с преступностью являются широко распространенной практикой среди органов национальной безопасности в государствах ЕС. В объединенных делах «Tele2Sverige» и «Уотсон (Watson) и другие» (C-203/15 и C-698/15, далее «Tele2») Суд ЕС постановил, что государства-члены не в праве обязывать поставщиков услуг электронной связи к общему и неизбирательному хранению данных. Это создало проблемы для государств-членов,

которые вследствие этого решения были лишены средства защиты национальной безопасности. На основании было возбуждено четыре отдельных дела в отношении законности предусмотренного национальным законодательством Великобритании, Франции и Бельгии требования в отношении поставщиков услуг электронной связи об общем и неизбирательном хранении данных. Ниже приводятся подробности разбирательства этих дел:

Дело C-623/17 (Соединенное Королевство)

5 июня 2015 года в Следственный трибунал Великобритании (Investigatory Powers Tribunal) британской правозащитной группой Privacy International был подан иск о незаконности законодательства, разрешающего получение и использование массивов коммуникационных данных службами безопасности и разведки (а именно британским Центром правительственной связи и британскими службами внутренней и внешней разведки (МИ-5 и МИ-6)). Примечательно, что в судебном решении от 17 октября 2016 года ответчики признали факт использования массивов персональных данных (таких как биографические данные, данные о поездках, финансовая, коммерческая информация и коммуникационные данные) в целях анализа путем перекрестной проверки и автоматизированной обработки, а также в целях их раскрытия другим лицам/органам власти и иностранным партнерам. Эти данные, полученные от сетей электронной связи общего пользования, использовались Центром правительственной связи и службой МИ-5 с 2001 и 2005 годов, соответственно.

Анализируя законность этих действий, Следственный трибунал установил, что меры по получению и использованию данных соответствовали национальному законодательству [п. 6 Решения 1]. Примечательно, что сети электронной связи были обязаны предоставлять службам безопасности и разведки данные, собранные в ходе своей экономической деятельности, однако это не касалось других данных, полученных этими службами без использования обязательных полномочий. Таким образом, суд счел целесообразным обратиться в Суд ЕС с вопросом о том, (а) подпадает ли национальный правовой режим под действие законодательства ЕС и (б) применимы ли к этому режиму требования, содержащиеся в «Tele2», и если да, то каким образом.

Дело C-511/18 (Франция)

30 ноября 2015 года и 16 марта 2016 года различные правозащитные группы и некоммерческие организации обратились в Государственный совет Франции с ходатайствами об аннулировании постановления, обязывавшего операторов электронной связи и поставщиков технических услуг «внедрить в своих сетях автоматизированные методы обработки данных, предназначенные ... для обнаружения связей, которые могут представлять террористическую угрозу» в соответствии с французским законодательством [стр. 25]. Заявители утверждали, что данные постановления нарушают Конституцию Франции, Европейскую конвенцию о защите прав человека и основных свобод (ЕКПЧ) и Директивы 2000/31 и 2002/58 (о защите персональных данных и конфиденциальности).

Рассматривавший дело суд пришел к выводу о том, что требование о хранении данных и доступ административных органов к этим данным подпадают под действие законодательства ЕС, однако счел, что оно не распространяется на положения национального законодательства, относящиеся непосредственно к методам сбора разведывательной информации, применяемым государством. Тем не менее, суд счел необходимым приостановить производство по делу и передал три вопроса для толкования в Суд ЕС.

Дело C-512/18 (Франция)

15 сентября 2016 года вышеупомянутые правозащитные группы подали отдельный иск против подразумеваемого решения об отказе в удовлетворении их ходатайства об отмене законодательных актов, которые якобы нарушали неприкосновенность частной жизни, налагая обязательство общего и неизбирательного хранения коммуникационных данных для судебных целей. Суд, рассматривавший дело, посчитал, что обязательство по хранению данных, примененное в данном деле, не подпадает под действие законодательства ЕС, поскольку сфера его действия ограничивается предоставлением общедоступных услуг электронной связи в сетях связи общего пользования на территории ЕС. Учитывая, что законодательство ЕС не устанавливает прямого запрета на хранение таких данных, суд также счел целесообразным передать это дело в Суд ЕС.

Дело C-520/18 (Бельгия)

В январе 2017 года в Конституционный суд Бельгии были поданы различные иски об отмене национального закона, предусматривающего требование о хранении данных. Заявители утверждали, что закон не обеспечивал адекватных гарантий защиты сохраняемых данных и создавал риск составления и неправомерного использования профилей личности компетентными органами. Они утверждали, что эти положения нарушают Конституцию Бельгии, некоторые положения ЕКПЧ, МПГПП (Международного пакта о гражданских и политических правах) и Договора о Европейском Союзе (ДЕС). Указывая на сходство между национальным законодательством Бельгии и законодательством ЕС о хранении данных, полученных в связи с использованием сетей связи общего пользования, Конституционный суд Бельгии решил передать дело в Суд ЕС для вынесения предварительного решения.

Решениями от 25 сентября 2018 года и 9 июля 2020 года Суд ЕС объединил дела C-511/18, C-512/18 и C-520/18. Дело C-623/17 рассматривалось отдельно. В трех отдельных заключениях от 15 января 2020 года Генеральный адвокат Кампос Санчес-Бордона постановил, что деятельность, осуществляемая государственными органами государств-членов ЕС по соображениям национальной безопасности и требующая сотрудничества со стороны частных лиц, не выходит за рамки Директивы 2002/58 о конфиденциальности и электронных средствах связи. Таким образом, положения Директивы (в частности, принцип конфиденциальности сообщений в соответствии со Статьей 5(1)) применимы в тех случаях, когда поставщики услуг электронной связи обязаны по закону сохранять данные и предоставлять доступ к ним государственным органам. По мнению Генерального адвоката, национальные режимы должны соответствовать стандартам Суда ЕС, установленным в делах «Tele2» и «Digital Rights Ireland и другие», C-293/12 и C-594/12 (далее «Digital Rights Ireland»), даже в случаях, связанных с национальной безопасностью.

Хотя государствам-членам разрешено принимать законодательные меры в интересах национальной безопасности, Генеральный адвокат также указал на необходимость «строгого» толкования ограничений, предусмотренных Статьей 5(1). Он рекомендовал ограничить хранение данных и доступ к ним целями эффективного предотвращения преступлений и обеспечения национальной безопасности, но также добавил, что в случаях существования непосредственной угрозы или чрезвычайного риска национальное законодательство вправе налагать общие и широкие обязательства по хранению данных [стр. 16 Заключения по делам C 511/18 и C 512/18]. Генеральный адвокат указал, что

обязательства по общему или неизбирательному хранению данных в связи с серьезными или постоянными угрозами национальной безопасности нарушают основные права, закрепленные в Хартии ЕС об основных правах. Утверждая, что борьба с терроризмом является вопросом не практической, а юридической эффективности [стр. 5 заключения по делу C 623/17], он заявил, что информирование субъектов данных является необходимым предварительным условием для сохранения данных, если только это не ставит под угрозу действия национальных властей.

Генеральный адвокат также заявил, что Директива не исключает сбор данных о трафике и местоположении в режиме реального времени, если он осуществляется в соответствии с установленными процедурами и гарантиями, упомянутыми выше. Это обязательство было признано применимым не только к тяжким преступлениям, но и к менее тяжким преступлениям, предусмотренным Статьей 23(1) Общего регламента [стр. 9 Заключения по делу C-520/18]. Что касается того, может ли национальный суд сохранить действие внутреннего закона в случае его несоответствия законодательству ЕС, Генеральный адвокат считает, что это возможно, только если сохранение действия этих законов оправдано и строго необходимо для устранения несоответствия законодательству ЕС.

Обзор решения

Большая палата Суда ЕС вынесла предварительное решение в двух постановлениях от 6 октября 2020 года. Основным вопросом, рассматриваемым Судом, была проблема применения Директивы о конфиденциальности и электронных средствах связи к деятельности, связанной с национальной безопасностью и борьбой с терроризмом. Суд ЕС сформулировал пять вопросов для рассмотрения:

Подпадает ли под действие Директивы 2002/58 национальное законодательство, позволяющее государственному органу требовать от поставщиков услуг электронной связи передавать данные службам безопасности и разведки в целях обеспечения национальной безопасности?

Должна ли Статья 15(1) Директивы 2002/58 толковаться как отменяющая национальное законодательство, обязывающее поставщиков услуг электронной связи сохранять

данные о трафике и местоположении в общем и неизбирательном порядке в целях, указанных в Статье 15(1)?

Должна ли статья 15(1) Директивы 2002/58 толковаться как отменяющая национальное законодательство, требующее от поставщиков услуг электронной связи применять в своих сетях меры, позволяющие осуществлять, во-первых, автоматизированный анализ и сбор данных о трафике и местоположении в режиме реального времени и, во-вторых, сбор технических данных о местоположении используемого оконечного оборудования в режиме реального времени без уведомления лиц, чьи данные подвергаются обработке и сбору? [п. 45]

Должны ли положения Директивы 2000/31 толковаться как отменяющие национальное законодательство, требующее от поставщиков услуг интернет-связи в сетях связи общего пользования и поставщиков услуг хостинга сохранять, в общем и неизбирательном порядке, персональные данные, относящиеся к этим услугам? [п. 49]

Может ли национальный суд применить положение национального законодательства, требующее общего и неизбирательного хранения данных о трафике и местоположении, в целях обеспечения национальной безопасности/борьбы с преступностью - несмотря на несовместимость законодательства со Статьей 15(1) Директивы 2002/58? [п. 52]

Статья 5(1) Директивы 2002/58 о конфиденциальности и электронных средствах связи закрепляет принцип конфиденциальности как электронных сообщений, так и связанных с ними данных о трафике, и предусматривает запрет на хранение этих сообщений и данных лицами, не являющимися пользователями, без согласия самих пользователей. Однако Статья 15(1) Директивы позволяет государствам-членам устанавливать исключения из этого принципа в соответствии со Статьей 5(1), если это необходимо для обеспечения национальной безопасности.

Что касается первого вопроса, Суд сначала постановил, что Директива 2002/58 о конфиденциальности и электронных средствах связи применима к национальному законодательству, требующему сбора и хранения персональных данных. Отрицательно ответив на утверждение ответчиков о том, что деятельность служб безопасности и разведки является важнейшей государственной функцией и, следовательно, исключительной ответственностью государств-членов, не подпадающей под действие Директивы, Суд ЕС постановил, что сфера действия Директивы распространяется не только на законодательные меры, требующие сбора и хранения данных, но и на законодательные меры, требующие от поставщиков услуг предоставления доступа к таким данным. Это объясняется тем, что такие законодательные меры требуют

обязательной обработки данных поставщиками услуг электронной связи и, следовательно, не могут рассматриваться как деятельность, присущая государствам. Ссылаясь на Общий регламент о защите данных (GDPR), Суд отметил, что раскрытие персональных данных путем передачи (например, хранение или предоставление доступа) представляет собой «обработку» (Общий регламент определяет понятие «обработка персональных данных» как любое действие или совокупность действий, совершаемых с персональными данными, включая сбор, хранение, использование, просмотр, раскрытие посредством передачи, распространение или иной вид предоставления доступа). [п. 15 дела C-623/17]

В противовес этому, Суд ЕС заявил, что единственным обстоятельством, при котором защита данных физических лиц не подпадает под действие законодательства ЕС, является случай, когда государства-члены применяют меры напрямую, без наложения на поставщиков услуг электронной связи обязательств по обработке данных.

После принятия решения о применимости Директивы 2002/58 к данной группе дел, суд изучил влияние права на безопасность, закрепленного в Статье 15(1) Директивы 2002/58 и Хартии основных прав ЕС (Статья 6 – «Право на свободу и безопасность»). В частности, суды, рассматривавшие дела, не были уверены в том, что хранение данных в соответствии с национальным законодательством противоречит статьям 7 («Уважение частной и семейной жизни») и 8 («Защита персональных данных») Хартии. Подтвердив решение по делам «Tele2» и «Уотсон (Watson) и другие», Суд ЕС постановил, что Директива 2002/58 не позволяет превращать в правило исключения из принципиального обязательства по обеспечению конфиденциальности электронных сообщений и связанных с ними данных и запрету на хранение таких данных (изложенные в Статье 5(1)). Следовательно, Суд пришел к выводу, что Директива не уполномочивает государства-члены принимать законодательные меры, ограничивающие объем прав в целях национальной безопасности, если только такие меры не соответствуют общим принципам права ЕС, таким как принцип соразмерности, и основным правам, гарантированным Хартией. [п. 35]

Важно отметить согласие Суда ЕС с тем, что возложение на поставщиков услуг электронной связи обязательств по хранению данных о трафике при помощи национального законодательства не только препятствует защите конфиденциальности и персональных данных, но и противоречит принципу свободы выражения мнения в соответствии со статьей 11 Устава ЕС. Суд не только подтвердил важность конфиденциальности и свободы выражения мнения при толковании статьи 11

Директивы, но и постановил, что хранение данных само по себе является отступлением от принципа конфиденциальности в соответствии со статьей 5(1), которая запрещает хранение данных любым лицам помимо пользователей. Суд счел неуместным проводить различие между конфиденциальными и неконфиденциальными данными или тем, использовались ли впоследствии сохраненные данные или нет.

Особое значение для Суда имел риск профилирования - возможность использования данных о трафике и местоположении для получения информации об аспектах частной жизни (таких как политические взгляды, сексуальная ориентация, религиозные убеждения, состояние здоровья, социальные отношения и т.д.) и составления точных выводов о частной жизни лиц, чьи данные были сохранены, представляла прямую угрозу праву на неприкосновенность частной жизни. В результате, Суд пришел к выводу о том, что, во-первых, хранение данных в полицейских целях само по себе является нарушением права на тайну сообщений, а во-вторых, само по себе хранение значительных объемов данных поставщиками услуг электронной связи влечет за собой риск злоупотреблений и незаконного доступа.

В этом контексте Суд ответил на второй вопрос утвердительно, постановив, что Директива ЕС отменяет национальное законодательство, обязывающее поставщиков услуг электронной связи осуществлять общую и неизбирательную передачу данных о трафике и местоположении службам безопасности и разведки с целью обеспечения национальной безопасности. Более того, Суд также заявил, что такое действие, даже в качестве превентивной меры, запрещено законодательством ЕС, особенно в отношении обязательств, предусматривающих хранение данных в общем или неизбирательном порядке и при отсутствии связи между поведением субъектов данных и целью, преследуемой рассматриваемым законодательством.

При этом Суд указал, что, если такое хранение оправдано в случае существования серьезной угрозы национальной или общественной безопасности, характер этой меры должен быть «строго» соразмерен ее предполагаемой цели. Эта цель может быть достигнута лишь в том случае, если она совместима с основными правами (толкование статьи 15(1)). Что еще более важно, Суд уточнил, что решение о вынесении такого постановления должно подлежать эффективному пересмотру либо Судом, либо независимым административным органом, уполномоченным выносить обязательные к исполнению решения. Суд также призвал разработать на национальном уровне четкие и ясные правила, регулирующие объем и применение хранения данных для защиты от риска злоупотреблений.

Однако Суд указал на различие в отношении хранения данных, касающихся гражданской идентификации пользователей систем электронной связи. Невозможность установления даты, времени, продолжительности и адресатов в таких случаях делает невозможным составление профиля частной жизни. Для такого целенаправленного хранения на основе объективных или неизбирательных факторов (в соответствии с категориями заинтересованных лиц или географическим критерием) законодательная мера, обязывающая поставщиков услуг электронной связи сохранять такие данные, допускается даже при отсутствии связи между всеми пользователями систем электронной связи и преследуемыми целями [п. 42]. Аналогичным образом допустимо хранение IP-адресов, присвоенных источнику связи, если оно ограничено строго необходимыми данными. Наконец, Директива не исключает применение законодательной меры при необходимости хранения данных сверх установленных законом сроков, когда факт правонарушения уже установлен или имеются обоснованные подозрения в отношении его существования.

По третьему вопросу Суд отметил, что автоматизированные методы сбора разведданных и сбор технических данных в режиме реального времени являются законными исключительно в целях предотвращения терроризма. В контексте толкования права Суд заявил, что данные, в отношении которых проводится автоматизированный анализ в целях проверки на терроризм, представляют собой «персональные данные» в соответствии с Общим регламентом, поскольку их все еще можно идентифицировать с конкретным лицом. На этом основании Суд пришел к выводу, что такой автоматизированный анализ данных о трафике и местоположении противоречит принципу конфиденциальности согласно Директиве 2002/58, а также основным правам согласно Хартии ЕС, и может оказать сдерживающее воздействие на осуществление свободы выражения мнения.

Доктрина «строгой» соразмерности применима даже в том случае, если вмешательство считается необходимым в связи с серьезной угрозой национальной безопасности. Для соблюдения требования о соразмерности необходимы следующие условия: (а) угроза национальной безопасности должна быть реальной и либо уже существующей, либо прогнозируемой, и (б) продолжительность хранения данных должна быть ограничена рамками строгой необходимости. Таким образом, заранее установленные модели или критерии для проведения автоматизированного анализа (такие как расовое или этническое происхождение, политические взгляды, религиозные или философские убеждения, членство в профсоюзе, информация о здоровье или сексуальной жизни

человека) с целью предотвращения терроризма сами по себе не могут основываться на конфиденциальных данных [п. 47]. Суд применил аналогичные рассуждения в отношении сбора персональных данных в режиме реального времени. Сбор таких данных не исключается Директивой, только если он ограничен лицами, которых есть веские основания подозревать в причастности к террористической деятельности, и подлежит предварительному рассмотрению судом или независимым административным органом.
Что касается четвертого вопроса, Суд истолковал статью 23(1) Общего регламента (которая предусматривает ограничения на обработку персональных данных) в совокупности с Хартией с целью отмены национального законодательства, требующего от поставщиков услуг интернет-связи в сетях связи общего пользования и поставщиков услуг хостинга сохранять, в общем и неизбирательном порядке, персональные данные, относящиеся к этим услугам. Суд применил выводы, сделанные в контексте вышеупомянутых вопросов, также и к статье 23 Общего регламента. Этот шаг был основан на принципе верховенства законодательства ЕС, который устанавливает приоритет законодательства ЕС над законодательством государств-членов. Однако Суд ЕС также постановил, что национальное законодательство должно определять правила, касающиеся приемлемости и оценки информации, полученной в результате хранения данных в нарушение законодательства ЕС, в уголовном процессе против подозреваемых лиц [п. 53]. Тем не менее, национальные уголовные суды обязаны игнорировать информацию или доказательства, полученные путем общего или неизбирательного хранения данных о трафике и местоположении в нарушение законодательства ЕС, если лица, подозреваемые в совершении уголовных преступлений, не могут эффективно прокомментировать эту информацию (на основании принципа эффективности). Таким образом, на последний вопрос Суд также ответил отрицательно.

ОРИЕНТАЦИЯ РЕШЕНИЯ

Итог: **расширяет сферу защиты права**

Массовая слежка оказывает расхолаживающее действие на защиту права на свободу слова. Решение Суда ЕС по данному делу является значительным шагом на пути к защите основных прав на свободу слова и выражение мнения в Европейском Союзе. Во всех

четырех случаях Суд использовал «строгий» контроль в качестве стандарта для законодательной деятельности, требующего от государств-членов осуществлять сбор и хранение данных только для удовлетворения неоспоримых государственных интересов, не связанных с подавлением идей. Это дело подтверждает, что обмен идеями и свободное выражение мнения являются позитивными и важными ценностями не только для тех, кто осуществляет свои права, но и для общества в целом.

ПЕРСПЕКТИВА

Перечень справочных документов

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

Соответствующее международное или региональное законодательство

ECJ, Tele2 Sverige AB v Post- och telestyrelsen, Secretary of State for the Home Department v Watson, Joined Cases C 203/15 and C 698/15 (2016)
ЕСПЧ, «Комиссия против Венгрии» (Commission v. Hungary) (Transparency of Associations) (2020), C-78/18.
ЕСПЧ, «К. Ю. Против Финляндии» (2008), жалоба № 2872/02.
ЕСПЧ, «Фон Ганновер (Von Hannover) против Германии» (2004), жалоба № 59320/00.
ЕСПЧ, М. К. Против Болгарии (2004), жалоба № 39272/98.
ЕСПЧ, «Осман (Osman) против Соединенного королевства» (1998), жалоба № 87/1997/871/1083.
ЕСПЧ, «Эль-Масри (El-Masri) против Бывшей Югославской Республики Македония» (2012), жалоба № 39630/09.
ЕСПЧ, «Медведев и другие против Франции» (2010), жалоба № 3394/03.
ЕСПЧ, «Ладент (Ladent) против Польши» (2008), жалоба № 11036/03.
ЕСПЧ, «Бен Файза (Ben Faiza) против Франции» (2018), жалоба № 31446/12.
CJEU, Commission v. Hungary (Rights of usufruct over agricultural land) (2019), C-235/17, EU:C:2019:432.
CJEU, Rayonna prokuratura Lom (2019), C-467/18, EU:C:2019:765.
CJEU, Digital Rights (2014), C-293/12 and C-594/12, EU:C:2014:238.
CJEU, Volker und Markus Schecke and Eifert (2010), C-92/09 and C-93/09, EU:C:2010:662.
CJEU, Satakunnan Markkinapörssi and Satamedia (2008), C-73/07, EU:C:2008:727.
CJEU, Ministerio Fiscal (2018), C-207/16, EU:C:2018:788.
CJEU, Facebook Ireland and Schrems (2020), C-311/18, EU:C:2020:55.
CJEU, SNB-REACT (2018), C-521/17, EU:C:2018:639.
CJEU, Mc Fadden (2016), C-484/14, EU:C:2016:689.
CJEU, SABAM (2012), C-360/10, EU:C:2012:85.
CJEU, Scarlet Extended (2011), C-70/10, EU:C:2011:771.
CJEU, Österreichischer Rundfunk and Others (2003), C-465/00, C-138/01 and C-139/01, EU:C:2003:294.
CJEU, Skype Communications (2019), C-142/18, EU:C:2019:460.

CJEU, Popławski (2019), C-573/17, EU:C:2019:530.
CJEU, Melki and Abdeli (2010), C-188/10 and C-189/10, EU:C:2010:363.
CJEU, A. K. and Others (Independence of the Disciplinary Chamber of the Supreme Court) (2019), C-585/18, C-624/18 and C-625/18, EU:C:2019:982.
CJEU, Flaminio Costa v E.N.E.L. (1964), Case 6/64, EU:C:1964:66.
CJEU, Inter-Environnement Wallonie and Bond BeterLeefmilieu Vlaanderen (2019), C-411/17, EU:C:2019:622.
CJEU, A and Others (Wind turbines at Aalter and Nevele) (2020), C-24/19, EU:C:2020:503.
CJEU, Nelson and Others (2020), C-581/10 and C-629/10, EU:C:2012:657.

ЗНАЧЕНИЕ

Решение создает обязательный или убедительный прецедент в рамках своей юрисдикции.

Решение (включая совпадающие и отличные мнения), создает обязательный или убедительный прецедент за рамками своей юрисдикции.

ОФИЦИАЛЬНЫЕ ДОКУМЕНТЫ ПО ДЕЛУ

- Судебное решение (на английском языке)
- Мнение Генерального адвоката по делам C-511/18 - 512/18, 15 января 2020 г.
- Мнение Генерального адвоката по делу C-520/18, 15 января 2020 г.
- Мнение Генерального адвоката по делу C-623/17

Доклады, аналитические и новостные статьи:

- **EU's top court blocks states from gathering user data for surveillance** https://www.ft.com/content/71cc07fb-58ff-404d-868c-5dd0e8a97e20
- **Ruling by EU's highest court finds that UK, French and Belgian mass surveillance regimes must respect privacy, even in the context of national security** https://privacyinternational.org/press-release/4205/press-release-ruling-eus-highest-court-finds-uk-french-and-belgian-mass
- **Q&A: EU's top court rules that UK, French and Belgian mass surveillance regimes must respect privacy** https://privacyinternational.org/long-read/4206/qa-eus-top-court-rules-uk-french-and-belgian-mass-surveillance-regimes-must-respect