



Сборник съдебна практика

Съединени дела C-511/18, C-512/18 и C-520/18

**La Quadrature du Net и др.
срещу
Premier ministre и др.**

(Преюдициални запитвания, отправени от Conseil d'État (Държавен съвет, Франция) и Cour constitutionnelle (Конституционен съд, Белгия)

Решение на Съда (голям състав) от 6 октомври 2020 година

„Преюдициално запитване — Обработване на лични данни в сектора на електронните съобщения — Доставчици на електронни съобщителни услуги — Доставчици на хостинг услуги и доставчици на достъп до интернет — Общо и неизбирателно запазване на данни за трафик и на данни за местонахождение — Автоматизиран анализ на данните — Достъп в реално време до данните — Защита на националната сигурност и борба с тероризма — Борба с престъпността — Директива 2002/58/ЕО — Приложно поле — Член 1, параграф 3 и член 3 — Поверителност на електронните съобщения — Защита — Член 5 и член 15, параграф 1 — Директива 2000/31/ЕО — Приложно поле — Харта на основните права на Европейския съюз — Членове 4, 6—8 и 11 и член 52, параграф 1 — Член 4, параграф 2 ДЕС“

1. *Сближаване на законодателствата — Сектор на далекосъобщенията — Обработване на лични данни и защита на неприкосновеността на личния живот в сектора на електронните съобщения — Директива 2002/58 — Приложно поле — Национална правна уредба, която налага на доставчиците на електронни съобщителни услуги задължение за запазване на данни за трафик и данни за местонахождение — Цели за защита на националната сигурност и борбата с престъпността — Включване (член 4, параграф 2 ДЕС; член 1, параграфи 1 и 3, член 3 и член 15, параграф 1 от Директива 2002/58 на Европейския парламент и на Съвета, изменена с Директива 2009/136)*

(вж. т. 92—96, 98—101, 103 и 104)

2. *Сближаване на законодателствата — Сектор на далекосъобщенията — Обработване на лични данни и защита на неприкосновеността на личния живот в сектора на електронните съобщения — Директива 2002/58 — Възможност за държавите членки да ограничат обхвата на определени права и задължения — Национални мерки, които налагат на доставчиците на електронни съобщителни услуги задължение за общо и неизбирателно запазване на данни за трафик и данни за местонахождение — Цел за защита на националната сигурност —*

Недопустимост — Национални мерки, които позволяват общо и неизбирателно запазване на тези данни в случай на тежка и непосредствена заплаха за националната сигурност — Допустимост — Национални мерки, които позволяват целево и бързо запазване за определен период на тези данни въз основа на обективни и недискриминационни критерии — Национални мерки, които предвиждат общо и неизбирателно запазване на IP адреси, дадени на източника на свързване с интернет за ограничен до строго необходимото период от време — Национални мерки, които предвиждат общо и неизбирателно запазване на данни относно самоличността на ползвателите на електронни съобщителни средства за неопределен период — Цел за защита на националната сигурност — Допустимост — Условия

(член 4, параграф 2 ДЕС; членове 7, 8 и 11 и член 52, параграф 1 от Хартата на основните права на Европейския съюз; член 5, параграф 1 и член 15, параграф 1 от Директива 2002/58 на Европейския парламент и на Съвета, изменена с Директива 2009/136)

(вж. т. 107, 109, 111—119, 122—128, 130—165 и 168; т. 1 от диспозитива)

3. *Сближаване на законодателствата — Сектор на далекосъобщенията — Обработване на лични данни и защита на неприкосновеността на личния живот в сектора на електронните съобщения — Директива 2002/58 — Възможност за държавите членки да ограничат обхвата на определени права и задължения — Национална правна уредба, която налага на доставчиците на електронни съобщителни услуги извършването на автоматизиран анализ и събирането в реално време на данни за трафик и данни за местонахождение — Допустимост — Условия*

(член 4, параграф 2 ДЕС; членове 7, 8 и 11 и член 52, параграф 1 от Хартата на основните права на Европейския съюз; член 5, параграф 1 и член 15, параграф 1 от Директива 2002/58 на Европейския парламент и на Съвета, изменена с Директива 2009/136)

(вж. т. 172—174, 175—182, 186—192; т. 2 от диспозитива)

4. *Сближаване на законодателства — Електронна търговия — Директива 2000/31 — Приложно поле — Защита на поверителността на съобщенията и на физическите лица при обработването на лични данни в рамките на услугите на информационното общество — Изключване — Приложимост според случая на Директива 2002/58 или на Регламент 2016/670*

(членове 7, 8, 11 и член 52, параграф 1 от Хартата на основните права на Европейския съюз; съображение 10 и член 23, параграфи 1 и 2 от Регламент 2016/679 на Европейския парламент и на Съвета; съображения 14 и 15 и член 1, параграфи 2 и 5, член 2, буква а) от Директива 2001/31 на Европейския парламент и на Съвета и член 5, параграф 1 и член 15, параграф 1 от Директива 2002/58 на Европейския парламент и на Съвета, изменена с Директива 2009/136)

(вж. т. 197—202, 204, 205, 207—212; т. 3 от диспозитива)

5. *Сближаване на законодателствата — Сектор на далекосъобщенията — Обработване на лични данни и защита на неприкосновеността на личния живот в сектора на електронните съобщения — Директива 2002/58 — Възможност за държавите членки да ограничат обхвата на определени права и задължения — Национални мерки, които налагат на доставчиците на електронни съобщителни услуги задължение за общо и неизбирателно запазване на данни за трафик и данни за местонахождение — Цел за защита на националната сигурност — Недопустимост — Отмяна от националния съд на мерки, които са несъвместими със задълженията, произтичащи от тази директива — Възможност за запазване на последиците на тези мерки — Условия — Неприложимост в случая — Последици, които трябва да се изведат от това за националния съд (членове 7, 8 и 11 и член 52, параграф 1 от Хартата на основните права на Европейския съюз; член 5, параграф 1 и член 15, параграф 1 от Директива 2002/58 на Европейския парламент и на Съвета, изменена с Директива 2009/136)*

(вж. т. 216—220, 223—228; т. 4 от диспозитива)

Резюме

Съдът на Европейския съюз потвърждава, че правото на Съюза не допуска национална правна уредба, която налага на доставчик на електронни съобщителни услуги задължение за общо и неизбирателно предаване или запазване на данни за трафик и на данни за местонахождение за целите на борбата с престъпността като цяло или на защитата на националната сигурност

Обратно, в случаи, в които държава членка е изправена пред сериозна заплаха за националната сигурност, която се оказва действителна и настояща или предвидима, същата може да допусне изключение от задължението да осигури поверителността на данните, свързани с електронните съобщения, като наложи чрез законодателни мерки общо и неизбирателно запазване на тези данни за ограничен до строго необходимото период от време, който може да бъде удължен, ако заплахата продължи да съществува.

Що се отнася до борбата с тежката престъпност и предотвратяването на сериозни заплахи срещу обществената сигурност, държава членка може също да предвиди целево запазване на посочените данни, както и тяхното бързо запазване. Подобна намеса в основните права трябва да бъде съпроводена от ефективни гаранции и да подлежи на контрол от съд или от независим административен орган. Освен това държавите членки могат да извършват общо и неизбирателно запазване на IP адресите, дадени на източника на съобщение, ако периодът на запазване е ограничен до строго необходимото, а също и да извършват общо и неизбирателно запазване на

данни относно самоличността на ползвателите на електронни съобщителни средства, без в последния случай то да е ограничено за определен срок

През последните години Съдът се произнася в редица решения относно запазването и достъпа до лични данни в областта на електронните съобщения¹. Съдебната практика, която произтича от тези решения, по-специално от решение *Tele2 Sverige и Watson и др.*, в което Съдът приема по-конкретно, че държавите членки не могат да налагат на доставчиците на електронни съобщителни услуги задължение за общо и неизбирателно запазване на данни за трафик и данни за местонахождение, поражда загрижеността на някои държави, опасяващи се, че са лишени от инструмент, който според тях е необходим за опазването на националната сигурност и за борбата с престъпността.

Именно на този фон *Investigatory Powers Tribunal* (Съд за контрол върху правомощията по разследване, Обединено кралство) (*Privacy International, C-623/17*), *Conseil d'État* (Държавен съвет, Франция) (*Le Quadrature du Net и др.*, съединени дела *C-511/18 и C-512/18*) и *Cour constitutionnelle* (Конституционен съд, Белгия) (*Ordre des barreaux francophones et germanophone и др.*, *C-520/18*) са сезирани със спорове относно законосъобразността на правните уредби, приети от някои държави членки в тези области, предвиждащи по-специално задължение на доставчиците на електронни съобщителни услуги общо и неизбирателно да предават на публичен орган или да запазват данните на потребителите относно трафика и местонахождението.

С две решения, постановени в голям състав на 6 октомври 2020 г., Съдът най-напред приема, че Директивата за правото на неприкосновеност на личния живот и електронни комуникации се прилага за национални правни уредби, които с цел опазване на националната сигурност и борбата с престъпността налагат на доставчиците на електронни съобщителни услуги задължение за обработване на лични данни, като например предаването им на публични органи или запазването им. Освен това, като потвърждава практиката си, установена с решение *Tele2 Sverige и Watson и др.*, относно непропорционалния характер на общото и неизбирателно запазване на данни за трафик и данни за местонахождение, Съдът внася уточнения, по-специално относно обхвата на правомощията, които тази директива признава на държавите членки в областта на запазването на такива данни за посочените по-горе цели.

¹ Така в решение от 8 април 2014 г., *Digital Rights Ireland и др.* (*C-293/12 и C-594/12, EU:C:2014:238*) (вж. пресъобщение № 54/14) Съдът обявява за невалидна Директива 2006/24/ЕО на Европейския парламент и на Съвета от 15 март 2006 година за запазване на данни, създадени или обработени, във връзка с предоставянето на обществено достъпни електронни съобщителни услуги или на обществени съобщителни мрежи и за изменение на Директива 2002/58/ЕО (ОВ L 105, стр. 54; Специално издание на български език, 2007 г., глава 13, том 53, стр. 51), с мотива че намесата в правото на зачитане на неприкосновеността на личния живот и правото на защита на личните данни, признати от Хартата на основните права на Европейския съюз (наричана по-нататък „Хартата“), която произтича от предвиденото в тази директива общо задължение за запазване на данни за трафик и данни за местонахождение, не е ограничена до строго необходимото. По-нататък, в решение от 21 декември 2016 г., *Tele2 Sverige и Watson и др.* (*C-203/15 и C-698/15, EU:C:2016:970*) (вж. пресъобщение № 145/16) Съдът тълкува член 15, параграф 1 от Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации) (ОВ L 201, 2002 г., стр. 37; Специално издание на български език, 2007 г., глава 13, том 36, стр. 63), изменена с Директива 2009/136/ЕО на Европейския парламент и на Съвета от 25 ноември 2009 година (ОВ L 337, 2009 г., стр. 11) (наричана по-нататък „Директива за правото на неприкосновеност на личния живот и електронни комуникации“). Тази разпоредба оправомощава държавите членки да приемат „законодателни мерки“, за да ограничат обхвата на определени предвидени в директивата права и задължения, от съображения за защита, включително на националната сигурност. Накрая, в решение от 2 октомври 2018 г., *Ministerio Fiscal* (*C-207/16, EU:C:2018:788*) (вж. пресъобщение № 141/18) Съдът тълкува същия член 15, параграф 1 по дело относно достъпа на публичните органи до данните относно самоличността на ползвателите на електронни съобщителни средства.

Най-напред, Съдът се погрижва да разсее повдигнатите в рамките на настоящите дела съмнения относно приложимостта на Директивата за правото на неприкосновеност на личния живот и електронни комуникации. Всъщност няколко държави членки, представили писмени становища пред Съда, заемат различни позиции в това отношение. Те изтъкват по-специално, че тази директива не се прилага по отношение на разглежданите национални правни уредби, тъй като те имат за цел опазването на националната сигурност, която попадала единствено в обхвата на тяхната компетентност, както свидетелствал по-специално член 4, параграф 2, трето изречение ДЕС. Съдът обаче счита, че национални правни уредби, които задължават доставчиците на електронни съобщителни услуги да запазват данни за трафик и данни за местонахождение или още да предават тези данни на националните органи за сигурност и разузнаване за тази цел, попадат в приложното поле на директивата.

По-нататък Съдът припомня, че Директивата за правото на неприкосновеност на личния живот и електронни комуникации² не позволява изключението от принципното задължение да се гарантира поверителността на електронните съобщения и свързаните с тях данни и от забраната за съхраняване на тези данни да се превръща в правило. Това означава, че тази директива позволява на държавите членки да приемат, включително и за целите на националната сигурност, законодателни мерки за ограничаване на обхвата на правата и задълженията, предвидени в тази директива, и по-специално на задължението за гарантиране на поверителността на съобщенията и на данните за трафика³, само при зачитане на общите принципи на правото на Съюза, сред които е принципът на пропорционалност, както и на основните права, гарантирани от Хартата⁴.

В този контекст Съдът приема, от една страна, по дело *Privacy International*, че Директивата за правото на неприкосновеност на личния живот и електронни комуникации, разглеждана във връзка с Хартата, не допуска национална правна уредба, която задължава доставчиците на електронни съобщителни услуги да предават на службите за сигурност и разузнавателните служби данни за трафик и данни за местонахождение с цел опазването на националната сигурност. От друга страна, по съединени дела *La Quadrature du Net* и др. и по дело *Ordre des barreaux francophones et germanophone* и др. Съдът счита, че същата директива не допуска законодателни мерки, които предвиждат задължение за доставчиците на електронни съобщителни услуги за превантивно общо и неизбирателно запазване на данни за трафик и данни за местонахождение. Всъщност тези задължения за общо и неизбирателно предаване и запазване на такива данни представляват особено сериозна намеса в основните права, гарантирани от Хартата, без поведението на лицата, чиито данни са засегнати, да има връзка с целта на разглежданата правна уредба. По аналогичен начин Съдът тълкува член 23, параграф 1 от Общия регламент относно защитата на данните⁵, разглеждан във връзка с Хартата, в смисъл, че не допуска национална правна уредба, която налага на доставчиците на достъп до обществени съобщителни услуги в интернет и на доставчиците на хостинг услуги задължение за общо и неизбирателно запазване по-специално на лични данни, свързани с тези услуги.

² Член 15, параграфи 1 и 3 от Директива 2002/58.

³ Член 5, параграф 1 от Директива 2002/58.

⁴ По-специално членове 7, 8 и 11 и член 52, параграф 1 от Хартата.

⁵ Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 2016 г., стр. 1).

Обратно, Съдът счита, че когато съответната държава членка е изправена пред сериозна заплаха за националната сигурност, която е действителна и настояща или предвидима, Директивата за правото на неприкосновеност на личния живот и електронни комуникации, разглеждана във връзка с Хартата, допуска да се разпорежи на доставчиците на електронни съобщителни услуги да извършват общо и неизбирателно запазване на данни за трафик и данни за местонахождение. В този контекст Съдът уточнява, че решението, което предвижда това разпореждане за период, ограничен до строго необходимото, трябва да подлежи на ефективен контрол от юрисдикция или от независима административна структура, чието решение има обвързващо действие, за да се провери дали е налице едно от тези положения, както и дали са спазени предвидените условия и гаранции. При същите условия посочената директива допуска и автоматизиран анализ на данните, и по-специално на данните за трафик и за местонахождение на всички ползватели на електронни съобщителни средства.

Съдът добавя, че Директивата за правото на неприкосновеност на личния живот и електронни комуникации, разглеждана в светлината на Хартата, допуска законодателни мерки, които позволяват целево запазване на данни за трафик и данни за местонахождение, което е ограничено въз основа на обективни и недискриминационни критерии в зависимост от категориите засегнати лица или посредством географски критерий, за период от време, ограничен до строго необходимото. Освен това тази директива допуска подобни мерки, които предвиждат общо и неизбирателно запазване на IP адреси, дадени на източника на съобщение, ако това запазване е за ограничен до строго необходимото период, както и мерки, предвиждащи подобно запазване на данни относно самоличността на ползвателите на електронни съобщителни средства, като в последния случай държавите членки не са длъжни да ограничават запазването във времето. В допълнение към това посочената директива допуска законодателна мярка, която позволява да се прибегне до бързо запазване на данните, с които разполагат доставчиците на услуги, в случаи, в които съществува необходимост от запазване на посочените данни след изтичане на законоустановените за запазването им срокове с цел разкриването на тежки престъпления или посегателства върху националната сигурност, когато тези престъпления или посегателства вече са били установени или когато може разумно да се подозира, че съществуват.

Освен това Съдът приема, че Директивата за правото на неприкосновеност на личния живот и електронни комуникации, разглеждана във връзка на Хартата, допуска национална правна уредба, която задължава доставчиците на електронни съобщителни услуги да събират в реално време по-специално данни за трафик и данни за местонахождение, когато това събиране е ограничено до лицата, за които съществува основателна причина да се подозира, че участват по един или друг начин в терористични дейности, и подлежи на предварителен контрол, осъществяван от юрисдикция или от независима административна структура, чието решение има обвързващо действие, за да се увери, че такова събиране в реално време е разрешено само в границите на строго необходимото. В спешни случаи контролът трябва да бъде осъществен в кратък срок.

Накрая, Съдът разглежда въпроса за запазването на последиците от национална правна уредба, за която е прието, че е несъвместима с правото на Съюза. В това отношение той приема, че национална юрисдикция не може да прилага разпоредба от националното си право, която я оправомощава да ограничи във времето действието на възложено ѝ обявяване на незаконосъобразност по отношение на национално законодателство, което налага на доставчиците на електронни съобщителни услуги общо и неизбирателно

запазване на данни за трафик и данни за местонахождение в разрез с Директивата за правото на неприкосновеност на личния живот и електронни комуникации, разглеждана във връзка с Хартата.

Като се има предвид това, за да се даде полезен отговор на националната юрисдикция, Съдът припомня, че допустимостта и преценката на доказателства, получени чрез запазване на данни в противоречие с правото на Съюза, в рамките на наказателно производство, образувано срещу лица, заподозрени в извършването на тежки престъпления, при сегашното състояние на правото на Съюза се уреждат единствено от националното право. Съдът обаче уточнява, че Директивата за правото на неприкосновеност на личния живот и електронни комуникации, тълкувана в светлината на принципа на ефективност, изисква националният наказателен съд да не взема предвид доказателства, получени чрез несъвместимо с правото на Съюза общо и неизбирателно запазване на данни за трафик и данни за местонахождение, в рамките на подобно наказателно производство, ако заподозрените в престъпни деяния лица не са в състояние да обсъдят ефективно тези доказателства.