Мерките в България и по света за ограничаване разпространението на заболяването COVID-19 поставят въпроса как следва да се обработват лични данни при извънредно положение за гарантиране спазване на наложени карантинни мерки. Безспорно, възможността за лесен достъп до данните на лицата позволява на правителствата да контролират населението и да ограничават разпространението на пандемията. Въпросът е, че тази информация може да бъде използвана и за редица други цели – като част от тези цели са несъвместими с изискванията на редица международни актове, които гарантират защитата на правото на личен живот.

Българската държава до момента демонстрира умереност – като предвиди възможност в Закона за електронните съобщения за целите на спазване на карантинните мерки да може да се достъпват данни от доставчиците на услуги относно ползваните от едно мобилно устройство клетки. Беше обявено, че е създадено и специално приложение за мобилни устройства, което да позволява от една страна по-лесен контрол върху лицата под карантина, а от друга – бърза връзка между всички лица и техните лични лекари. За момента това приложение вече е достъпно, но има малко информация относно начина на функционирането му, така че този анализ се основава на данните, оповестени от Министерски съвет.

Тези мерки станаха обект на критика – тъй като не предвиждат сериозни гаранции при достъп от властите до трафичните данни на лицата под карантина. За срока на извънредното положение тези данни могат да бъдат достъпвани само на основание искане от органите на полицията, без да е необходимо разрешение от съд – като доставчикът на услуги е задължен да предостави тези данни.

Тези критики не са изцяло основателни – мобилните устройства се оказват изключително ефективно средство за проследяване движението на техните ползватели, както е добре известно на различните доставчици на приложения и услуги. Затова и обикновено устройствата предават данни за своето местонахождение – често това се случва дори въпреки нежеланието на ползвателя. Затова гарантирането на достъп до тези данни за властите при необходимост от предприемане на мерки за опазване на общественото здраве изглежда съразмерно и логично. Опитът на редица държави като Китай и Южна Корея показва, че следенето

CR legal DL 2018. Всички права запазени.

на мобилни устройства гарантира успешен контрол върху спазването на мерките за карантина – и предотвратява разпространението на заразни заболявания.

Тази намеса в личния живот обаче трябва да е строго ограничена – за да не се превърне в тотален държавен контрол върху гражданите. Обработването на лични данни при извънредно положение може да бъде освободено от някои ограничения – но все пак трябва да бъдат зачитани основните стандарти, уредени например в Хартата на основните права на ЕС, Европейската конвенция за правата на човека и Общия регламент за защита на данните. Данните следва да се обработват само за целите на карантината, а всички изключения от стандартите за защита на личните данни да се прилагат само за периода на карантината.

В това отношение направените изменения в Закона за електронните съобщения изглежда обоснован – доколкото изключението от съдебния контрол е само за срока на извънредното положение. Събраните по този начин данни за евентуално неспазване на карантината ще могат освен това да са основание за ангажиране на отговорността на дадено лице само ако е спазена процедурата по събиране на тези данни – т.е. съдът ще има последващ контрол върху събирането и обработването. В този случай органите на изпълнителната власт носят отговорността да използват това средство за контрол само когато е крайно необходимо – и да докажат, че гласуваното им за срока на извънредното положение доверие е оправдано. А законодателната власт следва да не допуска разширяване на изключенията за случаи, които не са свързани с опазване на общественото здраве. Така може да бъде намерен баланс между правото на защита на лични данни при извънредно положение и необходимостта властите да могат да предприемат бързи и ефективни мерки.

Проблемът за баланса между правото на личен живот и необходимостта властите да разполагат с точни данни обаче излиза на преден план и при обявеното от Министерски съвет приложение ViruSafe. Приложението вече е достъпно, като за момента позволява да се въвеждат данни за симптоми – и може да получава данни за връзката на мобилното устройство с мрежите, съответно неговото местонахождение. Публикуваната информация обаче е изключително малко – и поставя редица въпроси.

CR legal DL 2018. Всички права запазени.

На първо място, може ли лицата под карантина да бъдат задължени да ползват това приложение? Към момента българското право не предвижда механизъм за такова задължение – а и е спорно до колко може да е ефективно, ако ползвателят не носи мобилното устройство със себе си. От друга страна, такова приложение може да е ефикасно при упражняването на контрол не само за целите на карантина, но и при изпълнение на мерки за неотклонение например.

На второ място, такова приложение може да събира повече данни отколкото само към коя клетка се свързва мобилното устройство. Тези данни могат да са много полезни – да позволяват например проследяване симптомите на лицето, здравното му състояние – но и се считат за чувствителни и са поставени под специална защита. Обработването на такива данни е подчинено на строги изисквания за контрол – и следва да се случва само когато е необходимо.

Приложението освен това ще позволява и лица, които не са под карантина да подават данни за своите симптоми – но не става ясно до кого ще стигат тези данни, как и за какъв срок ще се съхраняват и за какво ще могат да се ползват. Тук на преден план започват да излизат слабостите на създаденото приложение – тъй като то все още не е част от цялостна стратегия какво следва да се постигне със събираните данни. Този подход е изцяло в разрез със стандартите за защита на личните данни – тъй като означава централизиране на огромен масив от чувствителни данни, без да има яснота за какво ще се използват. Че приложение ще се намери, няма спор – може тези данни да служат за планиране на Националната здравна карта, за упражняване на контрол върху дейностите на лечебните заведения и т.н. – но процесът на целеполагане трябва да предхожда решението за събиране на лични данни. Особено когато събирането има възможност да продължи и след прекратяване на извънредното положение.

При създаването на масиви от данни освен това следва да бъде гарантирана и тяхната сигурност – тъй като след изтичането на лични данни от Националната агенция по приходите през 2019 г. мерките основно се свеждат до издирване на лицето, виновно за разгласяването на данните. Обаче издирването на това лице не е достатъчно, за да гарантира сигурността на другите масиви от информация, съхранявани от властите, нито ще помогне за възстановяване на щетите. Информация, веднъж споделена в

CR legal DL 2018. Всички права запазени.

интернет, трудно може да изчезне – и вредата, веднъж нанесена, трудно може да се поправи. Затова властите трябва да създадат доверие, че такива пробиви няма да се случат – а това предполага прилагане на мерки като децентрализиране на информацията, контрол на достъпа до нея, псевдонимизиране и т.н.

И не на последно място, създаването на приложение за обработване на тези данни предполага, че неговият разработчик ще има ангажимент за неговата поддръжка, а данните ще минават през мобилните устройства. Съответно трябва да се запитаме подходящо ли е всеки да има възможността да въвежда данните за здравословното си състояние без яснота до кого могат да достигнат? Факт е, че редица приложения вече събират такава информация, но властите трябва да бъдат особено внимателни – защото тяхната препоръка да се ползва дадено приложение може да има много сериозни последици. Затова създаването и ползването на такива приложения следва да е съобразено с много строги стандарти – и отношенията между държавата и създателя им да са прозрачни, така че да гарантират правата на лицата, които ще въвеждат своите данни.

В тази връзка вече има препоръка на Европейския надзорен орган по защита на данните, че ЕС следва да има едно централизирано приложение за обработване на този тип данни. Този подход може да спести някои от посочените проблеми – но все пак оставя отворени въпросите за какви цели ще се ползва тази информация, съответно как ще се гарантира нейната сигурност.

CR legal DL 2018. Всички права запазени.