Добре урядування: між свободою інформації та захистом даних

Інтерв'ю з Петером Шааром

Свобода інформації та захист даних мають дуже велику вагу в інформаційному суспільстві. Держава повинна йти назустріч громадянам із «піднятим забороло-м». Прозорість державної діяльності має бути правилом, зберігання таємниці — винятком. Ще одна невіддільна риса де-мократичної держави — дотримування основних прав на захист даних та інформаційне самови-значення.

Ви — фахівець із захисту даних, свободи інформації та інформаційного самовизначення. У чому Ви вбачаєте зв'язок між добрим урядуванням і відповідними вимогами, що їх висувають до урядів і адміністрацій?

Одна з рис доброго урядування — прозорість діяльності уряду. У демократичних умовах громадяни прагнуть знати, як і на підставі яких аргументів ухвалюють свої рішення органи влади. Уже багато років усі особи, що їх зачіпає діяльність адміністративних органів, можуть претендувати на ознайомлення зі своїми особовими справами. Але закони про захист даних обмежують таке право доступу лише даними, що стосуються конкретного заявника. Такого обмеженого права на інформування недостатньо. Тому за останні десятиліття практично в усіх демократичних країнах ухвалили закони про свободу інформації, які дають усім громадянам, не обов'язково фігурантам якихось справ, змогу ознайомлюватися з документами адміністративних органів або одержувати відповідні довідки. Однак добре урядування означає також, що діяльність державних органів має гарантувати дотримування основних громадянських прав. До основних прав у Німеччині та Європейському Союзі належать захист даних та інформаційне самовизначення.

Коли говорять про добре урядування, мова майже завжди заходить про прозорість. Але в контексті захисту даних ідеться також про сфери, інформацію з яких оприлюднювати які не можна. Як це поєднати?

Захист даних має кілька вимірів: гарантування права на приватність, інформаційне самовизначення та технічне регулювання. Стрімкий розвиток інформаційних технологій веде до того, що висвітлювати можна все більше сфер нашого життя. Усе складніші інформаційні технології впроваджують в усіх можливих виробах, від смартфона до динаміка, від тари для напоїв до автомобіля. Тим важливішими стають правові межі збирання, узагальнювання та аналізування даних. Захист даних у цьому контексті — не самоціль, а більше засіб гарантування вільного самовираження особистості. Той, хто знає, що всі його дії реєструють, почувається невільним і не може повною мірою користуватися своїми правами, такими як свобода думки або

право на демонстрації. Ті, хто збирає дані, передусім держава, мають обмежувати себе, адже перевищення міри в цьому порушує Основний закон. Усе важливішими стають автоматизовані процеси ухвалювання рішень і оцінювання ризиків на основі великих обсягів даних. І це також потребує правил. Найважливіше за все — прозоре розуміння того, з якими цілями, за якими правилами та методами обробляють дані. Прозорість і захист даних добре поєднуються.

Свобода інформації — один із наріжних каменів демократичної правової держави. Які стандарти чинні в Німеччині? Де можна сподіватися змін, ініційованих із європейського рівня?

Свобода інформації означає насамперед, що правило й виняток щодо таємності й прозорості міняють місцями. Традиційну службову таємницю підриває прагнення громадян знати, як працюють установи, хто і які рішення ухвалює, які особи та інституції долучаються до пошуку рішень. Федеральний закон про свободу інформації, ухвалений десь із десять років тому, задовольняє це прагнення лише частково. Законів про свободу інформації досі немає в деяких федеральних землях. Численні винятки з наявних законів про свободу інформації перешкоджають вільному доступу громадян до даних. Щоправда, деякі з винятків цілком обґрунтовані, наприклад, міркуваннями конфіденційності. Особлива проблема полягає в тому, що виробничі та комерційні таємниці — на відміну від персональних даних — підлягають цілковитому захисту. Але і на цій ниві потрібна рівновага між публічними інтересами щодо інформації та економічними інтересами підприємств, які виконують державні чи муніципальні замовлення. Дуже важливо також досягти в майбутньому такого становища, щоб установи інформували громадян не лише у відповідь на запити, але й також активно оприлюднювали незапитані дані. Оскільки всі, і адміністративні органи також, переходять на системи автоматизованого обробки даних, публікування доречної інформації в Інтернеті не потребуватиме великих додаткових витрат праці. Тому закон про свободу інформації слід удосконалити, перетворивши його на закон про прозорість. Деякі федеральні землі — насамперед землі-міста — випереджають у цьому інші.

Стосовно нових вимог до (внутрішньої) безпеки — де ви бачите найбільші небезпеки для права на вільний доступ до інформації та на конфіденційність?

Останніми роками служби безпеки масово отримують нові повноваження з нагляду. Відповідні закони все частіше оскаржують у Федеральному конституційному суді та Європейському суді. Найбільшу, з мого погляду, проблему становить збирання даних про осіб, яких ні в чому не підозрюють, — нагромаджування даних «наперед», наприклад, за допомогою все ширшої відеореєстрації, яку ще й доповнюють технологіями розпізнавання облич. Тут потрібні чіткі межі, щоб ми не закінчили тотальним контролем, який несумісний із демократичним верховенством права. Є негаразди й щодо вільного доступу до інформації Наприклад, новинні агентства не підпадають під дію закону про свободу інформації. У Німеччині, на відміну від США тощо, громадяни взагалі не мають права вимагати від них якихось даних. Тому й у цій сфері потрібна більша прозорість.

Яким, на Вашу думку, має бути ідеальний захист «викривачів»?

Захист викривачів у Німеччині далеко не досконалий, зокрема як порівняти з іншими європейськими країнами. Ті, хто заявляє або прилюдно повідомляє про порушення закону підприємствами або установами, мають бути захищені від негативних наслідків. Найважливіші в цьому контексті «телефони довіри», за якими можна анонімно викривати порушників.

Як забезпечувати конфіденційність у наші часи небувалого розвитку інформаційно-комунікаційних технологій? Чи це в інтересах адміністрацій та інших державних органів? Чому?

Вороття в аналогові часи не буде. Саме тому важливо встановити чіткі правила застосовування інформаційних технологій. Захист даних та інформаційна безпека — ключові передумови, без яких люди не довірятимуть свої дані підприємствам і установам. Гідні довіри системи й відповідальне поводження з даними — не лише вимоги правової держави, але й також стратегічні чинники стрімкого оцифровування (диджиталізації) нашого суспільства. Верховенство права, основні права та права людини мають бути забезпечені й за нових умов.

Петер Шаар (Peter Schaar)

Із 2003 по 2013 Петер Шаар обіймав посаду Федерального вповноваженого із захисту даних і свободи інформації. Нині він — голова Європейської академії свободи інформації та захисту даних у Берліні.

Контакт

Європейська Академія Берліна
Bismarckallee 46/48
D-14193 Berlin-Grunewald (Берлін)
Т.: +49 30 8959510
eab@eab-berlin.eu
www.eab-berlin.eu