ČLANAK 29 RADNA STRANA ZA ZAŠTITU PODATAKA

00.264 / 10 / HR
WP 169

†

Mišljenje 1/2010 o konceptima "kontrolor" i "procesor"

Usvojen 16. veljače 2010

SADRŽAJ

Sažetak

Koncept kontrolora podataka i njegova interakcija s konceptom procesora podataka imaju ključnu ulogu u primjeni Direktive 95/46 / EZ, budući da određuju tko će biti odgovoran za poštivanje pravila o zaštiti podataka, kako subjekti podataka mogu ostvariti svoja prava , što je primjenjivo nacionalno pravo i kako učinkovito djeluju tijela za zaštitu podataka.

Organizacijska diferencijacija u javnom i privatnom sektoru, razvoj ICT-a, kao i globalizacija obrade podataka, povećavaju složenost načina na koji se obrađuju osobni podaci i zahtijevaju pojašnjenja tih koncepata, kako bi se osigurala učinkovita primjena i usklađenost praksa.

Pojam kontrolor je autonomna, u smislu da bi se trebala tumačiti uglavnom u skladu sa zakonom o zaštiti podataka Zajednice i funkcionalnim, u smislu da je namijenjena raspodjeli odgovornosti tamo gdje je činjenični utjecaj, a time i na temelju činjenične, a ne formalne analize.

Definicija u Direktivi sadrži tri glavna elementa:
- osobni aspekt ("*fizičku ili pravnu osobu, javno tijelo, agenciju ili bilo koje drugo tijelo*„);
- mogućnost pluralističke kontrole ("*koji sami ili zajedno s drugima*");
- bitne elemente za razlikovanje kontrolora od drugih sudionika ("*određuje svrhu i način obrade osobnih podataka*„).

Analiza ovih sastavnih dijelova dovodi do niza zaključaka koji su sažeti u stavku IV.

Ovo mišljenje također analizira koncept procesor, čije postojanje ovisi o odluci kontrolora, koja može odlučiti da li će obraditi podatke unutar svoje organizacije ili delegirati sve ili dio aktivnosti obrade vanjskoj organizaciji. Dva osnovna uvjeta za kvalificiranje obrađivača su, s jedne strane, zasebna pravna osoba u odnosu na kontrolora i, s druge strane, obrađuju osobne podatke u njegovo ime.

Radna skupina prepoznaje poteškoće u primjeni definicija Direktive u složenom okruženju, gdje se mogu predvidjeti mnogi scenariji koji uključuju kontrolore i procesore, sami ili zajedno, s različitim stupnjevima autonomije i odgovornosti.

U svojoj analizi naglasio je potrebu da se odgovornost raspodijeli na način da će se poštovanje pravila o zaštiti podataka u praksi u dovoljnoj mjeri osigurati. Međutim, on nije našao nikakav razlog da smatra da trenutna razlika između kontrolora i obrađivača više neće biti relevantna i izvodljiva u tom pogledu.

Radna skupina stoga se nada da će objašnjenja dana u ovom mišljenju, ilustrirana konkretnim primjerima iz svakodnevnog iskustva tijela za zaštitu podataka, pridonijeti učinkovitom usmjeravanju na način tumačenja tih temeljnih definicija Direktive.

Radna skupina za zaštitu pojedinaca u pogledu obrade osobnih podataka

uspostavljene Direktivom 95/46 / EZ Europskog parlamenta i Vijeća od 24. listopada 1995.

uzimajući u obzir članke 29. i 30. stavak 1. točku (a) i članak 3. te Direktive i članak 15. stavak 3. Direktive 2002/58 / EZ Europskog parlamenta i Vijeća od 12. srpnja 2002.,

uzimajući u obzir svoj Poslovnik,

usvojio je sljedeće mišljenje:

I. Uvod

Koncept kontrolora podataka i njegova interakcija s konceptom obrade podataka imaju ključnu ulogu u primjeni Direktive 95/46 / EZ, budući da određuju tko će biti odgovoran za poštivanje pravila o zaštiti podataka i kako subjekti podataka mogu ostvariti svoje prava u praksi. Koncept kontrolora podataka također je bitan za određivanje primjenjivog nacionalnog prava i učinkovito izvršavanje nadzornih zadaća dodijeljenih tijelima za zaštitu podataka.

Stoga je od iznimne važnosti da je točno značenje ovih koncepata i kriterija za njihovu ispravnu uporabu dovoljno jasno i da ih dijele svi oni u državama članicama koji igraju ulogu u provedbi Direktive iu primjeni, ocjeni i provedbi nacionalnih odredbi koje ga primjenjuju.

Postoje naznake da može postojati nedostatak jasnoće, barem što se tiče nekih aspekata ovih koncepata, i nekih različitih pogleda među praktičarima u različitim državama članicama koji mogu dovesti do različitih tumačenja istih načela i definicija uvedenih u svrhu usklađivanja na europskoj razini. Zbog toga je Radna skupina iz članka 29. odlučila, kao dio svog strateškog programa rada za razdoblje 2008.-2009., Posvetiti posebnu pozornost izradi dokumenta kojim se utvrđuje zajednički pristup tim pitanjima.

Radna skupina priznaje da konkretna primjena koncepata kontrolora podataka i procesora podataka postaje sve složenija. To je uglavnom zbog sve veće složenosti okruženja u kojem se ti koncepti koriste, a posebno zbog rastuće tendencije, kako u privatnom tako iu javnom sektoru, prema organizacijskoj diferencijaciji, u kombinaciji s razvojem ICT-a i globalizacije. na način koji može dovesti do novih i teških pitanja i ponekad može rezultirati nižom razinom zaštite koja se pruža subjektima podataka.

Iako su odredbe Direktive formulirane na tehnološki neutralan način i do sada su se mogle dobro oduprijeti razvoju konteksta, te složenosti doista mogu dovesti do neizvjesnosti u pogledu raspodjele odgovornosti i opsega primjenjivih nacionalnih zakona. Te nesigurnosti mogu imati negativan učinak na poštivanje pravila o zaštiti podataka u kritičnim područjima i na učinkovitost zakona o zaštiti podataka u cjelini. Radna skupina se već bavila nekim od tih pitanja

u odnosu na specifična pitanja[1], ali smatra da je sada potrebno dati više razvijene smjernice i posebne smjernice kako bi se osigurao dosljedan i usklađen pristup.

Stoga je Radna skupina odlučila dati u ovom mišljenju - na sličan način kao što je već učinjeno u Mišljenju o konceptu osobnih podataka[2] - neka pojašnjenja i neki konkretni primjeri[3] u odnosu na koncepte kontrolora podataka i procesora podataka.

II. Opća zapažanja i pitanja politike

Direktiva izričito upućuje na koncept kontrolora u nekoliko odredbi. Definicije „kontrolor" i „obrađivač" u članku 2. točkama (d) i (e) Direktive 95/46 / EZ (daljnja „Direktiva") glase kako slijedi:

> *"Kontrolor" znači fizička ili pravna osoba, javno tijelo, agencija ili bilo koje drugo tijelo koje samostalno ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka; ako su svrhe i sredstva obrade određeni nacionalnim zakonima ili propisima Zajednice, kontrolor ili posebni kriteriji za njegovo imenovanje mogu biti određeni nacionalnim pravom ili pravom Zajednice;*

> *"Procesor" znači fizička ili pravna osoba, javno tijelo, agencija ili drugo tijelo koje obrađuje osobne podatke u ime kontrolora*

Te su definicije oblikovane tijekom pregovora o nacrtu prijedloga za Direktivu početkom 1990-ih, a pojam „kontrolor" u osnovi je preuzet iz Konvencije Vijeća Europe 108 zaključene 1981. godine. Tijekom tih pregovora došlo je do nekih važnih promjena.

Prije svega, 'kontrolor spisa' u Konvenciji 108 zamijenjen je 'kontrolor' u odnosu na 'obradu osobnih podataka'. To je širok pojam, definiran u članku 2. točki (b) Direktive kao „svaka operacija ili skup operacija koje se obavljaju na temelju osobnih podataka, neovisno o tome jesu li automatskim sredstvima ili ne, kao što su prikupljanje, bilježenje, organizacija, pohrana, prilagodba ili izmjena, pronalaženje, savjetovanje, korištenje, objavljivanje putem prijenosa, širenja ili na drugi način dostupnog, usklađivanja ili kombiniranja, blokiranja, brisanja ili uništenja. " Koncept „kontrolora" se stoga više nije koristio za statični objekt („datoteka"), već se odnosio na aktivnosti koje odražavaju životni ciklus informacija od prikupljanja do njegovog uništenja, a to je trebalo promatrati i detaljno iu njegova cjelovitost ('rad ili skup operacija'). Iako je rezultat mogao biti isti u mnogim slučajevima, koncept je time dobio mnogo širi i dinamičniji smisao i opseg.

---

1 Vidjeti npr. Mišljenje 10/2006 o obradi osobnih podataka od strane Društva za svjetske međubankovne financijske telekomunikacije (SWIFT), usvojenog 22. studenog 2006. (WP 128), i nedavno Mišljenje 5/2009 o online društvenim mrežama, usvojeno 12. lipnja 2009 (WP 163).

2 Mišljenje 4/2007 o konceptu osobnih podataka, usvojeno 20. lipnja 2007. (WP 136)

3 Ti primjeri temelje se na trenutnoj nacionalnoj ili europskoj praksi i možda su izmijenjeni ili dopunjeni kako bi se osiguralo bolje razumijevanje.

Druge promjene uključivale su uvođenje mogućnosti "pluralističke kontrole" ("same ili zajedno s drugima"), uvjet da kontrolor "odredi svrhe i sredstva obrade osobnih podataka", te ideju da je to određivanje nacionalnim ili pravom Zajednice ili na drugi način. Direktiva je također uvela koncept „prerađivača", koji se ne spominje u Konvenciji 108. Te i druge promjene detaljnije će se analizirati tijekom ovog mišljenja.

II.1. Uloga koncepata

Dok koncept kontrolera (datoteke) igra vrlo ograničenu ulogu[4] u Konvenciji 108, to je potpuno drugačije u Direktivi. Članak 6. stavak 2. izričito propisuje da „kontrolor mora osigurati da se poštuje stavak 1.". To se odnosi na glavna načela koja se odnose na kvalitetu podataka, uključujući načelo iz članka 6. stavka 1. točke (a) da „osobni podaci moraju biti obrađeni pošteno i zakonito". To znači da su sve odredbe koje postavljaju uvjete za zakonitu obradu bitno upućene kontroloru, čak i ako to nije uvijek jasno izraženo.

Nadalje, odredbe o pravima subjekta podataka, na informacije, pristup, ispravak, brisanje i blokiranje, te na prigovor na obradu osobnih podataka (članci 10-12 i 14), uokvirene su na takav način da stvoriti obveze za kontrolora. Kontrolor je također ključan u odredbama o obavješćivanju i prethodnoj provjeri (članci 18-21). Konačno, ne bi trebalo biti iznenađenje da je kontrolor također načelno odgovoran za svaku štetu koja je posljedica nezakonite obrade (članak 23.).

To znači da prije svega uloga koncepta kontrolera utvrditi tko je odgovoran za poštivanje pravila o zaštiti podataka i kako subjekti podataka mogu u praksi ostvarivati svoja prava.[5] Drugim riječima: to dodijeliti odgovornost

To je u središtu Direktive, čiji je prvi cilj "zaštititi pojedince u pogledu obrade osobnih podataka". Taj se cilj može ostvariti i učiniti djelotvornim u praksi, ako se oni koji su odgovorni za obradu podataka mogu dovoljno potaknuti pravnim i drugim sredstvima da poduzmu sve mjere koje su potrebne kako bi se osigurala ta zaštita u praksi. To je potvrđeno u članku 17. stavku 1. Direktive, prema kojem kontrolor "*mora provesti odgovarajuće tehničke i organizacijske mjere zaštititi osobne podatke od slučajnog ili nezakonitog uništavanja ili slučajnog gubitka, izmjene, neovlaštenog otkrivanja ili pristupa, osobito ako obrada uključuje prijenos podataka putem mreže, i protiv svih drugih nezakonitih oblika obrade*„.

---

4 On se ne koristi ni u jednoj od temeljnih odredbi, osim u članku 8.a u odnosu na pravo na informiranje (načelo transparentnosti). Kontrolor kao odgovorna strana vidljiv je samo u određenim dijelovima memoranduma.

5 Vidi također uvodnu izjavu 25. Direktive 95/46 / EZ: „*Budući da se načela zaštite moraju odražavati, s jedne strane, u obvezama koje se nameću osobama, javnim tijelima, poduzećima, agencijama ili drugim tijelima odgovornim za obradu, posebno u pogledu kvalitete podataka, tehničke sigurnosti, obavijesti nadzornom tijelu i okolnosti pod kojima se može izvršiti obrada i, s druge strane, u pravu koja se dodjeljuje pojedincima, o podacima o kojima je predmet obrade, da se obavijesti da se odvija obrada, da se konzultiraju podaci, zatraže korekcije, pa čak i prigovor na obradu u određenim okolnostima*„.

Sredstva za poticanje odgovornosti mogu biti proaktivna i reaktivna. U prvom slučaju, oni trebaju osigurati učinkovitu primjenu mjera zaštite podataka i dostatna sredstva za odgovornost kontrolora. U drugom slučaju, oni mogu uključivati građansku odgovornost i sankcije kako bi se osiguralo da se svaka relevantna šteta nadoknadi i da se poduzmu odgovarajuće mjere za ispravljanje pogrešaka ili pogrešnih radnji.

Koncept kontrolera je također bitan element u određivanju koji se nacionalni zakon primjenjuje na operaciju obrade ili skup operacija obrade. Glavno pravilo primjenjivog prava prema članku 4. stavku 1. točki (a) Direktive je da svaka država članica primjenjuje svoje nacionalne odredbe na „*obrada osobnih podataka, gdje (...) provodi u kontekstu aktivnosti osnivanja kontrolora na teritoriju države članice*". Ova odredba se nastavlja na sljedeći način:*kada isti kontrolor je uspostavljen na teritoriju nekoliko država članica, on mora poduzeti potrebne mjere kako bi to osigurao svakoj od tih ustanova ispunjava obveze koje propisuje mjerodavno nacionalno pravo*". To znači da je ustanova (-e) kontrolora (-a) također odlučujuća za primjenjivo nacionalno (-e) zakonodavstvo (-a), a možda i za niz različitih primjenjivih nacionalnih zakona i načina na koji se oni odnose jedni na druge.[6]

Konačno, treba napomenuti da se pojam kontrolora pojavljuje u mnogim različitim odredbama Direktive kao element njihovog djelokruga ili posebnog uvjeta koji se primjenjuju na temelju njih: npr. Članak 7. propisuje da se osobni podaci mogu obrađivati samo ako: "*(c) obrada je nužna radi poštivanja zakonske obveze na koju kontroler (e) obrada je potrebna za izvršavanje zadatka koji se obavlja u javnom interesu ili u izvršavanju službenih ovlasti kontroler ili u trećoj osobi kojoj je datum otkriven, ili (f) obrada je potrebna za svrhe legitimnih interesa kojima teži kontroler ili od strane treće strane ili stranaka kojima se podaci otkrivaju, osim ako su ti interesi nadjačani ...* ". Identitet kontrolora također je važan element informacija subjektu podataka koji se zahtijeva prema člancima 10. i 11. \ t

pojam "procesora" igra važnu ulogu u kontekstu povjerljivosti i sigurnosti obrade (članci 16-17), budući da služi za utvrđivanje odgovornosti onih koji su bliže uključeni u obradu osobnih podataka, bilo pod izravnim ovlaštenjem kontrolora ili drugdje u njegovo ime. Razlika između „kontrolora" i „obrađivača" uglavnom služi za razlikovanje onih koji su odgovorni kao kontrolor (i) i onih koji djeluju samo u njihovo ime. To je opet uglavnom pitanje kako dodijeliti odgovornost Druge posljedice, bilo u smislu primjenjivog zakona ili na neki drugi način, mogu teći odatle.

Međutim, u slučaju prerađivača, postoji daljnja posljedica - i za kontrolora i za obrađivača - u smislu članka 17. Direktive mjerodavno pravo za sigurnost obrade nacionalno pravo države članice u kojoj je prerađivač osnovan.[7]

□ □

6 Radna skupina namjerava usvojiti posebno mišljenje o "primjenjivom zakonu" tijekom 2010. godine. Kada institucije i tijela Zajednice obrađuju osobne podatke, procjena kontrolinga je također relevantna s obzirom na moguću primjenu Uredbe (EZ) 45/2001 ili drugih relevantnih pravnih instrumenata EU-a.

7 Vidjeti članak 17. stavak 3. druga alineja: „obveza […] kako je definirana zakonom države članice u kojoj je poslovni subjekt osnovan, također je dužan obrađivati".

Konačno, kako je definirano u članku 2 (f),*treća strana "znači svaka fizička ili pravna osoba, javno tijelo, agencija ili bilo koje drugo tijelo, osim subjekta podataka, kontrolor, obrađivač i osobe koje su, pod izravnim ovlaštenjem kontrolora ili obrađivača, ovlaštene za obradu podaci*„. Kontrolor i procesor i njihovo osoblje stoga se smatraju „unutarnjim krugom obrade podataka" i nisu obuhvaćeni posebnim odredbama o trećim stranama.

II.2. Relevantan kontekst

Različiti razvoji u relevantnom okruženju učinili su ova pitanja hitnijima i složenijima nego prije. U vrijeme potpisivanja Konvencije 108 i, u velikoj mjeri, kada je usvojena Direktiva 95/46 / EZ, kontekst obrade podataka još je uvijek bio relativno jasan i jasan, ali to više nije slučaj.

To je prije svega zbog rastuće tendencije ka organizacijskoj diferencijaciji u većini relevantnih sektora. U privatnom sektoru, raspodjela financijskih ili drugih rizika dovela je do stalne korporativne diverzifikacije, koja je samo pojačana spajanjima i akvizicijama. U javnom sektoru slična se diferencijacija odvija u kontekstu decentralizacije ili odvajanja odjela za politiku i izvršnih agencija. U oba sektora sve je veći naglasak na razvoju lanaca isporuke ili pružanja usluga u različitim organizacijama te na korištenje podugovaranja ili eksternalizacije usluga kako bi se iskoristila specijalizacija i moguće ekonomije razmjera. Kao rezultat toga, dolazi do porasta raznih usluga koje pružaju pružatelji usluga, koji se ne smatraju uvijek odgovornima ili odgovornima. Zbog organizacijskih izbora tvrtki (i njihovih izvođača ili podizvođača) relevantne baze podataka mogu biti smještene u jednoj ili više zemalja unutar ili izvan Europske unije.

Razvoj informacijskih i komunikacijskih tehnologija ("ICT") uvelike je olakšao ove organizacijske promjene i dodao nekoliko vlastitih. Odgovornosti na različitim razinama - često rezultat organizacijske diferencijacije - obično zahtijevaju i potiču opsežnu uporabu ICT-a. Razvoj i implementacija ICT proizvoda i usluga također dovodi do novih uloga i odgovornosti u vlastitom pravu, koje nisu uvijek jasno povezane s postojećim ili razvijanjem odgovornosti u organizacijama klijenata. Stoga je važno biti svjestan relevantnih razlika i po potrebi pojasniti odgovornosti. Uvođenje mikro-tehnologije - kao što su čipovi RFID-a u potrošačke proizvode - postavlja slična pitanja prijenosa odgovornosti. S druge strane, postoje nova i teška pitanja koja se odnose na korištenje distribuiranog računalstva, osobito "računalstva u oblaku" i "mreža".[8]

Globalizacija je još jedan komplicirajući čimbenik. Tamo gdje organizacijska diferencijacija i razvoj ICT-a uključuju višestruke nadležnosti, kao što je često oko Interneta, pitanja primjenjivog prava se moraju pojaviti, ne samo unutar EU-a ili EEA-a, nego iu odnosu na treće zemlje. Ilustracija se može naći u okviru antidoping konteksta, gdje Svjetska antidoping agencija (WADA), osnovana u Švicarskoj, upravlja bazom podataka koja uključuje informacije o sportašima (ADAMS) kojima se upravlja iz Kanade u suradnji s nacionalnim anti- doping organizacijama diljem svijeta

[8] 'Računanje u oblaku' je vrsta računalstva u kojoj se skalabilne i elastične IT mogućnosti pružaju kao usluga za više korisnika koji koriste internetske tehnologije. Tipične usluge računalstva u oblaku pružaju uobičajene poslovne aplikacije na mreži kojima se pristupa putem web-preglednika, dok se softver i podaci pohranjuju na poslužiteljima. U tom smislu oblak nije otok nego globalni spoj svjetskih informacija i korisnika. Što se tiče "rešetki", vidi dolje primjer 19.

svijet. WP29 je istaknuo podjelu odgovornosti i pripisivanje kontrolinga kao izazove specifičnih poteškoća.[9]

To znači da središnja pitanja u ovom mišljenju imaju visok stupanj praktične važnosti i mogu imati velike posljedice.

II.3. Neki ključni izazovi

U smislu ciljeva Direktive, najvažnije je osigurati da. \ T odgovornost za obradu podataka Jasno određeno i može biti učinkovito

Ako nije dovoljno jasno što se od koga traži - npr. Nitko nije odgovoran ili mnoštvo mogućih kontrolora - postoji očigledan rizik da će se premalo, ako ništa, dogoditi i da će zakonske odredbe ostati neučinkovite. Također je moguće da će nejasnoće u tumačenju dovesti do konkurentnih potraživanja i drugih kontroverzi, u kojem slučaju će pozitivni učinci biti manji od očekivanog ili se mogu smanjiti ili nadmašiti nepredviđenim negativnim posljedicama.

U svim tim slučajevima ključni je izazov osigurati dovoljnu jasnoću kako bi se omogućila i osigurala učinkovita primjena i poštivanje u praksi U slučaju sumnje, rješenje koje će najvjerojatnije promicati takve učinke može biti poželjna opcija.

Međutim, isti kriteriji koji pružaju dovoljnu jasnoću također mogu dovesti do dodatne složenosti i neželjenih posljedica. Na primjer, razlikovanje kontrole, u skladu s organizacijskim stvarnostima, može dovesti do složenosti u primjenjivom nacionalnom pravu, gdje su uključene različite nadležnosti.

Analiza bi stoga trebala oštro pratiti razliku između prihvatljivih posljedica prema sadašnjim pravilima i moguću potrebu za prilagodbom postojećih pravila kako bi se osigurala kontinuirana učinkovitost i izbjeglo nepotrebne posljedice u promjenjivim okolnostima.

To znači da je sadašnja analiza od velike strateške važnosti i treba je primjenjivati oprezno iu punoj svijesti o mogućim međusobnim vezama između različitih pitanja.

III.

Analiza definicija

III.1. Definicija kontrolera

Definicija kontrolora u Direktivi sadrži tri glavna elementa, koji će se analizirati zasebno za potrebe ovog mišljenja. One su sljedeće:

- "Fizička ili pravna osoba, javno tijelo, agencija ili bilo koje drugo tijelo"
- "Koji sam ili zajedno s drugima"
- "Određuje svrhu i sredstva obrade osobnih podataka".

[9] Mišljenje br. 3/2008 od 1. kolovoza 2008. o nacrtu Međunarodnog standarda za zaštitu privatnosti Svjetskog antidoping kodeksa, WP156

Prvi sastavni dio odnosi se na osobni aspekt definicije. Treći blok sadrži bitne elemente za razlikovanje kontrolora od drugih aktera, dok drugi blok razmatra mogućnost 'pluralističke kontrole'. Ti su blokovi usko povezani. Međutim, radi metodologije koju treba slijediti u ovom mišljenju, svaka od ovih stavki će se rješavati odvojeno.

Za praktične svrhe, korisno je početi s *prvi element* trećeg građevnog bloka - tj. značenja riječi "određuje" - i nastaviti s ostatkom trećeg bloka, i tek tada obraditi prvi i drugi blok.

III.1.a) Preliminarni element: "određuje"

Kao što je već spomenuto, koncept kontrolora imao je malu ulogu u Konvenciji 108. U skladu s člankom 2. Konvencije, "kontrolor spisa" definiran je kao tijelo "tko jest" kompetentan ... odlučiti". Konvencija naglašava potrebu za kompetencijom koja se određuje "prema nacionalnom zakonu". Stoga je Konvencija upućivala na nacionalne zakone o zaštiti podataka, koji bi, u skladu s memorandumom o objašnjenju, sadržavali "precizne kriterije za određivanje tko je nadležna osoba".

Iako prvi prijedlog Komisije odražava tu odredbu, izmijenjeni prijedlog Komisije umjesto toga upućuje na tijelo "koje odlučuje", čime se eliminira potreba da se nadležnost za odlučivanje utvrdi zakonom: definicija zakonom je još uvijek moguća, ali nije potrebna. To se zatim potvrđuje Zajedničkim stajalištem Vijeća i usvojenim tekstom, koji se odnose na tijelo koje određuje.

U tom kontekstu, povijesni razvoj ističe dva važna elementa: prvo, da je moguće biti kontrolor bez obzira posebne nadležnosti ili ovlasti za kontrolu podataka dodijeljenih zakonom; drugo, da u procesu donošenja Direktive 95/46 određivanje kontrolora postaje koncept Zajednice, koncept koji ima svoje samostalan značenje u pravu Zajednice, ne mijenjajući se zbog - vjerojatno divergentnih - odredbi nacionalnog prava. Ovaj posljednji element nužan je kako bi se osigurala učinkovita primjena Direktive i visoka razina zaštite u državama članicama, što zahtijeva ujednačeno i stoga autonomno tumačenje takvog ključnog pojma kao "kontrolor", koji u Direktivi stječe značaj koji nije imao u Konvenciji 108.

U toj perspektivi, Direktiva dovršava ovaj razvoj tako što utvrđuje da, čak i ako sposobnost da se "utvrdi" može proizaći iz posebnog pripisivanja propisanog zakonom, to obično proizlazi iz analize faktičan elementi ili okolnosti slučaja: treba razmotriti konkretne operacije obrade i razumjeti tko ih određuje, tako što će u prvom stupnju odgovoriti na pitanja "zašto se odvija ta obrada?" Tko ga je pokrenuo?

Biti kontrolor prvenstveno je posljedica činjeničnih okolnosti koje je subjekt odlučio obraditi osobne podatke za svoje potrebe. Doista, samo formalni kriterij ne bi bio dovoljan barem iz dva razloga: u nekim slučajevima formalno imenovanje kontrolora - propisano na primjer zakonom, u ugovoru ili u obavijesti tijelu za zaštitu podataka - samo bi nedostaje; u drugim slučajevima, može se dogoditi da formalno imenovanje ne odražava stvarnost, formalno povjeravajući ulogu kontrolora tijelu koje zapravo nije u poziciji "odrediti".

Relevantnost činjeničnog utjecaja također je prikazana u slučaju SWIFT-a[10], gdje je SWIFT formalno smatran obrađivačom podataka, ali je de facto djelovao - barem u određenoj mjeri - kao kontrolor podataka. U tom je slučaju jasno da iako određivanje stranke kao kontrolora podataka ili obrađivača u ugovoru može otkriti relevantne informacije o pravnom statusu te stranke, takva ugovorna oznaka ipak nije presudna u određivanju njezina stvarnog statusa, mora se temeljiti na konkretnim okolnostima.

Ovaj činjenični pristup također je potkrijepljen razmatranjem da direktiva utvrđuje da je kontrolor onaj koji "određuje" umjesto "zakonito određuje" svrhu i sredstva. Učinkovita identifikacija kontrolinga je odlučujuća, čak i ako se čini da je oznaka nezakonita ili se obrada podataka vrši na nezakonit način. Nije relevantno je li odluka o obradi podataka bila "zakonita" u smislu da je subjekt koji donosi takvu odluku bio pravno sposoban to učiniti, ili da je kontrolor formalno imenovan u skladu s posebnim postupkom. Pitanje zakonitosti obrade osobnih podataka i dalje će biti relevantno u drugoj fazi i bit će ocijenjeno u svjetlu drugih članaka (osobito članaka 6-8) Direktive. Drugim riječima, važno je osigurati da čak iu slučajevima kada se podaci obrađuju nezakonito, kontrolor može lako pronaći i smatrati odgovornim za obradu.

Posljednja značajka koncepta kontrolera je njegova autonomija, u smislu da, iako vanjski pravni izvori mogu pomoći u utvrđivanju tko je kontrolor, treba ga tumačiti uglavnom prema zakonu o zaštiti podataka.[11] Koncept kontrolora ne bi trebao biti narušen drugim - ponekad sudarajućim ili preklapajućim - konceptima u drugim područjima prava, kao što su tvorac ili nositelj prava intelektualnog vlasništva. Biti nositelj prava na intelektualno vlasništvo ne isključuje mogućnost da se kvalificira i kao "kontrolor" i stoga podliježe obvezama koje proizlaze iz zakona o zaštiti podataka.

Potreba za tipologijom

Koncept kontrolera je a funkcionalna koncept, namijenjen raspodijeliti odgovornosti tamo gdje je činjenični utjecaj, a time i na činjeničnoj, a ne formalnoj analizi Stoga određivanje kontrole ponekad može zahtijevati detaljnu i dugotrajnu istragu. Međutim, potreba da se osigura djelotvornost zahtijeva poduzimanje pragmatičnog pristupa s ciljem osiguranja predvidljivost s obzirom na kontrolu. U tom pogledu, potrebna su pravila i praktične pretpostavke za usmjeravanje i pojednostavljenje primjene zakona o zaštiti podataka.

To zahtijeva tumačenje Direktive kojom se osigurava da se "odlučujuće tijelo" može lako i jasno identificirati u većini situacija, pozivajući se na one - pravne i / ili činjenične - okolnosti iz kojih se obično može utvrditi činjenični utjecaj, osim ako drugi elementi ne ukazuju na to upravo suprotno.

---

[10] Slučaj se odnosi na prenošenje bankovnih podataka prikupljenih od strane SWIFT-a američkim vlastima, u cilju borbe protiv financiranja terorizma, u cilju obavljanja financijskih transakcija u ime banaka i financijskih institucija.

[11] Vidi infra, smetnje s konceptima koji postoje u drugim područjima prava (na primjer, koncept nositelja prava na intelektualno vlasništvo ili znanstveno istraživanje, ili odgovornost u skladu s građanskim pravom).

Te okolnosti mogu se analizirati i klasificirati prema sljedećim trima kategorijama situacija koje omogućuju sustavan pristup tim pitanjima:

1) *Kontrola koja proizlazi iz izričite pravne nadležnosti* Ovo je *između ostalog* slučaj naveden u drugom dijelu definicije, tj. kada je kontrolor ili posebni kriteriji za njegovo imenovanje određeni nacionalnim pravom ili pravom Zajednice. Izričito imenovanje kontrolora po zakonu nije uobičajeno i obično ne predstavlja velike probleme. U nekim zemljama, nacionalnim zakonom propisano je da su tijela javne vlasti odgovorna za obradu osobnih podataka u kontekstu njihovih dužnosti.

Međutim, češći je slučaj kada zakon, umjesto da izravno imenuje kontrolora ili odredi kriterije za njegovo imenovanje, uspostavlja zadatak ili nameće dužnost nekome da prikuplja i obrađuje određene podatke. Primjerice, to bi bio slučaj s subjektom kojem su povjereni određeni javni zadaci (npr. Socijalno osiguranje) koji se ne mogu ispuniti bez prikupljanja barem nekih osobnih podataka, te uspostavlja registar s ciljem njihovog ispunjavanja. U tom slučaju iz zakona proizlazi tko je kontrolor. Općenito, zakon može nametnuti obvezu javnim ili privatnim subjektima da zadrže ili pruže određene podatke. Ti bi se subjekti tada normalno smatrali kontrolorima za svaku obradu osobnih podataka u tom kontekstu.

2) *Kontrola koja proizlazi iz implicitne kompetencije* To je slučaj kada sposobnost određivanja nije izričito propisana zakonom, niti izravna posljedica izričitih zakonskih odredbi, ali još uvijek proizlazi iz zajedničkih zakonskih odredbi ili uspostavljene pravne prakse koja se odnosi na različita područja (građansko pravo, trgovačko pravo, radno pravo). , itd.). U tom slučaju, postojeće tradicionalne uloge koje obično podrazumijevaju određenu odgovornost pomoći će u identifikaciji kontrolora: na primjer, poslodavac u odnosu na podatke o svojim zaposlenicima, izdavaču u odnosu na podatke o pretplatnicima, udruga u odnosu na podatke o svojim članovima ili suradnika.

U svim tim slučajevima, sposobnost određivanja aktivnosti obrade može se smatrati prirodno vezanom uz funkcionalnu ulogu (privatne) organizacije, koja u konačnici podrazumijeva odgovornosti i sa stajališta zaštite podataka. U pravnom smislu, to bi se primjenjivalo bez obzira na to da li će sposobnost za određivanje biti dodijeljena spomenutim pravnim tijelima, koju će izvršavati odgovarajući organi koji djeluju u njihovo ime, ili fizička osoba u sličnoj ulozi (vidi dalje u tekstu prvi element u točki c). Međutim, isto bi vrijedilo i za javno tijelo s određenim administrativnim poslovima, u zemlji u kojoj zakon ne bi bio eksplicitan u pogledu njegove odgovornosti za zaštitu podataka.

Primjer br. 1: Telekom operateri

Zanimljiv primjer pravnog usmjeravanja privatnog sektora odnosi se na ulogu telekomunikacijski operatori: Uvodna izjava 47 Direktive 95/46 / EZ pojašnjava da "*gdje poruka koja sadrži osobne podatke prenosi se putem telekomunikacija ili usluga elektroničke pošte, čija je jedina svrha prijenos takvih poruka, kontrolor u odnosu na osobne podatke sadržane u poruci obično će biti smatra se osobom od koje potječe poruka, a ne osobom pružanje usluga prijenosa; (...) ipak, oni koji nude takve usluge će obično se smatraju kontrolorima u pogledu obrade dodatnih osobne podatke potrebne za rad usluge "*. Davatelj usluga telekomunikacijske usluge bi se stoga u načelu trebale smatrati kontrolorima samo za podatke o prometu i naplati, a ne za podatke koji se prenose[12] Ovo je legalno smjernice zakonodavca Zajednice u potpunosti su u skladu s funkcionalnošću pristup u ovom mišljenju.

3) *Kontrola koja proizlazi iz činjeničnog utjecaja* To je slučaj kada se odgovornost kao kontrolor pripisuje na temelju procjene činjeničnih okolnosti. U mnogim slučajevima to će uključivati procjenu ugovornih odnosa između različitih uključenih strana. Ova procjena omogućuje izradu vanjskih zaključaka, dodjeljivanje uloge i odgovornosti kontrolora jednoj ili više stranaka. To bi moglo biti osobito korisno u kompliciranim okruženjima, često koristeći nove informacijske tehnologije, gdje su relevantni akteri često skloni da sebe vide kao "facilitatore", a ne kao odgovorne kontrolore.

Može se dogoditi da ugovor ne govori o tome tko je kontrolor, ali sadrži dovoljno elemenata za dodjelu odgovornosti kontrolora strani koja očito ima dominantnu ulogu u tom pogledu. Može također biti da je ugovor jasniji u odnosu na kontrolora. Ako nema razloga sumnjati da to točno odražava stvarnost, ne postoji ništa protiv poštivanja uvjeta ugovora. Međutim, uvjeti ugovora nisu odlučujući u svim okolnostima, jer bi to samo omogućilo strankama da dodijele odgovornost tamo gdje smatraju da je prikladno.

Sama činjenica da netko određuje kako se obrađuju osobni podaci može uključivati kvalifikaciju kontrolora podataka, čak i ako se ta kvalifikacija pojavljuje izvan opsega ugovornog odnosa ili je izričito isključena ugovorom. Jasan primjer za to bio je slučaj SWIFT, kojim je ova tvrtka donijela odluku o stavljanju na raspolaganje određenih osobnih podataka - koji su izvorno obrađeni u komercijalne svrhe u ime financijskih institucija - također u svrhu borbe protiv financiranja terorizma, kako je zatražio sudske pozive koje su izdale SAD Riznica.

[12] DPA se bavila kontrolom u predmetu koji je pokrenuo subjekt koji se žali na neželjeno oglašavanje putem e-pošte. Svojom je pritužbom subjekt podataka zatražio od pružatelja komunikacijske mreže da potvrdi ili poriče da je to pošiljatelj oglašivačke e-pošte. Agencija za zaštitu autorskih prava izjavila je da tvrtka koja klijentu pruža samo pristup komunikacijskoj mreži, tj. Ni pokretanje prijenosa podataka niti odabir adresata niti mijenjanje informacija sadržanih u prijenosu, ne može se smatrati kontrolorom podataka.

U slučaju sumnje, drugi elementi od uvjeta ugovora mogu biti korisni za pronalaženje kontrolora, kao što je stupanj stvarne kontrole koju provodi stranka, slika data subjektima podataka i razumna očekivanja subjekata podataka na temelju toga vidljivost (vidi također i treći element u točki b). Ova kategorija je posebno važna jer omogućuje da se bave i raspodjele odgovornosti iu onim slučajevima nezakonitog ponašanja, gdje se stvarne aktivnosti obrade mogu čak provoditi protiv interesa i spremnosti nekih strana.

Preliminarni zaključak

Među tim kategorijama, prva dva dopuštaju načelno sigurniju naznaku odlučujućeg tijela i mogu pokriti više od 80% relevantnih situacija u praksi. Međutim, formalna pravna oznaka trebala bi biti u skladu s pravilima o zaštiti podataka, osiguravajući da imenovano tijelo ima stvarnu kontrolu nad postupcima obrade, odnosno drugim riječima, da zakonsko imenovanje odražava stvarnost stvari.

Kategorija 3 zahtijeva složeniju analizu i vjerojatnije je da će dovesti do divergentnih tumačenja. Uvjeti ugovora često mogu pomoći razjasniti problem, ali nisu odlučujući u svim okolnostima. Postoji sve veći broj aktera koji sebe ne smatraju određivanjem aktivnosti obrade i stoga odgovorni za njih. Zaključak na temelju činjeničnog utjecaja je u tim slučajevima jedina moguća opcija. Pitanje zakonitosti ove obrade i dalje će se ocjenjivati u svjetlu drugih članaka (6-8).

Ako nijedna od gore navedenih kategorija nije primjenjiva, imenovanje kontrolora trebalo bi smatrati "ništavim". Zapravo, tijelo koje nema pravni niti činjenični utjecaj kako bi odredilo kako se obrađuju osobni podaci ne može se smatrati kontrolorom.

S formalne perspektive, razmatranje koje potkrjepljuje ovaj pristup jest da definiciju kontrolora podataka treba smatrati obveznom pravnom odredbom, iz koje stranke ne mogu jednostavno odstupiti ili odstupiti. Iz strateške perspektive, takvo bi imenovanje bilo u suprotnosti s učinkovitom primjenom zakona o zaštiti podataka i poništilo bi odgovornost koju sadrži obrada podataka.

III.1.b) Treći element: "svrhe i sredstva obrade"

Treći element predstavlja bitan dio testa: što bi stranka trebala odrediti kako bi se kvalificirala kao kontrolor.

Povijest ove odredbe pokazuje mnoge promjene. Konvencija br. 108 odnosila se na svrhu automatiziranih datoteka, kategorije osobnih podataka i operacije koje se na njih primjenjuju. Komisija je uzela te suštinske elemente, uz manje izmjene jezika, i dodala nadležnost da odluči koje treće strane mogu imati pristup podacima. Izmijenjeni prijedlog Komisije učinio je korak naprijed u prelasku s "svrhe datoteke" na "svrhe i ciljeve obrade", prelazeći iz statičke definicije povezane s datotekom na dinamičku definiciju povezanu s djelatnošću obrade. Izmijenjeni prijedlog i dalje se odnosio na četiri elementa (svrha / cilj, osobne podatke, operacije i treće strane koje imaju pristup njima), koje su smanjene na dvije ("svrhe i sredstva") samo zajedničkim stajalištem Vijeća.

Rječnici definiraju “svrhu” kao “očekivani ishod koji je namijenjen ili koji usmjerava vaše planirane akcije” i “znači” kao “kako je rezultat dobiven ili je postignut kraj”.

S druge strane, Direktiva to utvrđuje podaci moraju biti prikupljene za određene, eksplicitne i legitimne svrhe, a ne dalje se obrađivati na način koji nije u skladu s tim ciljevima. Određivanje "svrhe" obrade i "sredstva" za njihovo postizanje stoga je posebno važno.

Može se također reći da određivanje svrhe i sredstava predstavlja određivanje "zašto" i "kako" određenih aktivnosti obrade. U toj perspektivi, uzimajući u obzir da oba elementa idu zajedno, postoji potreba za pružanjem smjernica o tome stupanj utjecaja na "zašto" i "kako" mogu sadržavati kvalifikaciju subjekta kao kontrolora.

Kada je riječ o procjeni određivanje svrhe i sredstava s ciljem pripisivanja uloge kontrolora podataka, Stoga je ključno pitanje kome razina detalja netko bi trebao odrediti svrhu i sredstva kako bi se smatrao kontrolorom. I u korelaciji s tim, što je granica manevra što dopušta Direktiva za procesora podataka Ove definicije postaju osobito relevantne kada su razni sudionici uključeni u obradu osobnih podataka, a potrebno je odrediti koji od njih je kontrolor podataka (sam ili zajedno s drugima) i koji se umjesto toga smatraju procesorima podataka - ako ih ima.

Naglasak koji se stavlja na svrhu ili sredstva može varirati ovisno o specifičnom kontekstu u kojem se odvija obrada.

Potreban je pragmatičan pristup, stavljajući veći naglasak na diskreciju u određivanju svrhe i na slobodu donošenja odluka. U tim slučajevima, pitanje je zašto se procesiranje događa i kakva je uloga mogućih povezanih aktera kao što su outsourcing tvrtke: bi li vanjska tvrtka obradila podatke ako ih kontrolor nije pitao i pod kojim uvjetima? Procesor može djelovati dalje prema općim smjernicama koje se uglavnom pružaju u svrhe i ne ulaze duboko u detalje u pogledu sredstava.

Primjer br. 2: Mail marketing

Tvrtka ABC sklapa ugovore s različitim organizacijama kako bi izvršila svoju poštu marketinške kampanje i pokrenuti platni spisak. To daje jasne upute (što marketing materijal za slanje i kome, te kome platiti, koji iznosi, do kojeg datuma itd.).
Iako organizacije imaju određenu diskreciju (uključujući koji softver koristiti) njihovi zadaci su prilično jasni i čvrsto definirani i iako poštanska kuća može nude savjet (npr. savjetovanje protiv slanja poruka u kolovozu) koje su jasno vezane djelovati kao ABC. Štoviše, samo jedan subjekt, tvrtka ABC, ima pravo koristiti podatke koji se obrađuju - svi drugi subjekti moraju se osloniti na pravnu osnovu tvrtke ABC ako je njihova pravna sposobnost obrade podataka upitna. U ovom slučaju Jasno je da je tvrtka ABC kontrolor podataka i svaki od njih organizacije mogu se smatrati procesorom u pogledu specifične obrade podataka u njegovo ime.

Što se tiče određivanja sredstava, pojam “sredstva” očito obuhvaća vrlo različite vrste elemenata, što je također ilustrirano poviješću te definicije.

U izvornom prijedlogu uloga kontrolora proizlazi iz utvrđivanja četiriju elemenata (svrha / cilj, osobni podaci, operacije i treće strane koje imaju pristup njima). Konačna formulacija odredbe, koja se odnosi samo na "svrhe i sredstva", ne može se tumačiti kao da je u suprotnosti sa starijom verzijom, budući da ne može biti sumnje u činjenicu da npr. Kontrolor mora odrediti koji će se podaci obraditi za predviđene namjene. Stoga se konačna definicija mora shvatiti samo kao skraćena verzija koja ipak sadrži smisao starije verzije. Drugim riječima, "sredstvo" ne odnosi se samo na tehničke načine obrade osobnih podataka, već i na "način" obrade, što uključuje pitanja poput "koji podaci će se obrađivati", "koje treće strane imaju pristup te podatke ”,“ kada se podaci brišu ”, itd.

Određivanje "sredstava" stoga uključuje i tehnička i organizacijska pitanja u kojima se odluka može dobro delegirati procesorima (npr. "Koji hardver ili softver će se koristiti?") I bitne elemente koji su tradicionalno i inherentno rezervirani za određivanje kontrolor, kao što su "koji se podaci obrađuju?", "koliko dugo će se obraditi?", "tko će im pristupiti?", i tako dalje.

U tom kontekstu, dok bi određivanje svrhe obrade u svakom slučaju potaknulo kvalifikaciju kao kontrolora, utvrđivanje sredstava podrazumijevalo bi kontrolu samo kada se određivanje odnosi na bitne elemente sredstava.

U tom smislu, moguće je da tehnička i organizacijska sredstva određuju isključivo obrađivači podataka.

U tim slučajevima - kada postoji dobra definicija svrhe, ali malo ili čak nikakvih smjernica o tehničkim i organizacijskim sredstvima - sredstva bi trebala predstavljati razuman način postizanja svrhe (a) i kontrolor podataka trebao bi biti u potpunosti informiran o sredstvima koristi. Da li bi izvoditelj mogao utjecati na svrhu i izvršiti obradu (također) za vlastitu korist, na primjer korištenjem osobnih podataka primljenih s ciljem stvaranja usluga s dodanom vrijednošću, bio bi kontrolor (ili možda zajednički kontrolor)) za drugu aktivnost obrade i stoga podliježe svim obvezama primjenjivog zakona o zaštiti podataka.

Primjer br. 3: Tvrtka se naziva procesor podataka, ali djeluje kao kontrolor

Tvrtka MarketinZ pruža usluge promotivnog oglašavanja i izravnog marketinga različitim tvrtkama. Tvrtka GoodProductZ sklapa ugovor s MarketinZ-om, prema kojem potonja tvrtka osigurava komercijalno oglašavanje za korisnike GoodProductZ-a i naziva se procesor podataka. Međutim, MarketinZ odlučuje koristiti bazu podataka klijenata GoodProducts i za svrhu promicanja proizvoda drugih kupaca. Ova odluka o dodavanju dodatne svrhe onoj za koju su osobni podaci preneseni pretvara MarketinZ u kontrolora podataka za ovu obradu. Pitanje zakonitosti ove obrade i dalje će se ocjenjivati u svjetlu drugih članaka (6-8).

U nekim pravnim sustavima osobito su važne odluke koje se donose o sigurnosnim mjerama, budući da se sigurnosne mjere izričito smatraju ključnom karakteristikom koju treba definirati kontrolor. Time se postavlja pitanje koje odluke o sigurnosti mogu podrazumijevati kvalifikaciju kontrolora za tvrtku kojoj je izvršena obrada.

Preliminarni zaključak

Određivanje "svrhe" obrade rezervirano je za "kontrolora". Tko god donese takvu odluku, dakle (*zapravo*) kontroler. Određivanje „sredstava" obrade može delegirati kontrolor, što se tiče tehničkih ili organizacijskih pitanja. Značajna pitanja koja su bitna za jezgru zakonitosti obrade rezervirana su za kontrolora. Osoba ili subjekt koji odlučuje npr. O tome koliko dugo će podaci biti pohranjeni ili koji će imati pristup obrađenim podacima djeluje kao 'kontrolor' u vezi s ovim dijelom korištenja podataka i stoga mora ispunjavati sve obveze kontrolora.

III.1.c) Prvi element: "fizička osoba, pravna osoba ili bilo koje drugo tijelo"

Prvi element definicije odnosi se na osobnu stranu: tko može biti kontrolor i stoga se smatra krajnje odgovornim za obveze koje proizlaze iz Direktive. Definicija odražava upravo formulaciju članka 2. Konvencije 108 i nije bila predmetom konkretne rasprave u procesu donošenja odluka u Direktivi. Odnosi se na široki niz tema, koje mogu igrati ulogu kontrolora, od prirodnih do pravnih osoba i uključujući "bilo koje drugo tijelo".

Važno je da tumačenje ovog elementa osigura učinkovita primjena Direktive, u najvećoj mogućoj mjeri daje jasnu i jednoznačnu identifikaciju kontrolora u svim okolnostima, bez obzira je li formalno imenovanje izvršeno i objavljeno

Prije svega, važno je ostati što bliže praksi koja je uspostavljena iu javnom iu privatnom sektoru prema drugim pravnim područjima, kao što su građansko, upravno i kazneno pravo. U većini slučajeva ove odredbe ukazuju na to koje odgovornosti ili osobe treba dodijeliti i koje će u načelu pomoći da se utvrdi tko je kontrolor podataka.

U strateškoj perspektivi raspodjele odgovornosti, te kako bi se subjektima podataka omogućio stabilniji i pouzdaniji referentni entitet za ostvarivanje njihovih prava prema Direktivi, prednost treba dati procjeni tvrtke ili tijela kao kontrolora radije nego određenu osobu unutar tvrtke ili tijela. Za obradu podataka i obveze koje proizlaze iz zakonodavstva o zaštiti podataka, smatrat će se odgovorna tvrtka ili tijelo, osim ako ne postoje jasni elementi koji ukazuju na to da je fizička osoba odgovorna. Općenito, treba pretpostaviti da je poduzeće ili javno tijelo kao takvo odgovorno za aktivnosti obrade koje se odvijaju u okviru djelatnosti i rizika.

Ponekad tvrtke i javna tijela imenuju određenu osobu odgovornu za provedbu operacija obrade. Međutim, iu slučaju kada je određena fizička osoba imenovana kako bi se osigurala usklađenost s načelima zaštite podataka ili za obradu osobnih podataka, on / ona neće biti kontrolor, već će djelovati u ime pravne osobe (tvrtke ili javnog tijela) , koji će i dalje biti odgovorni u slučaju kršenja načela u svojstvu kontrolora.[13]

Posebno za velike i složene strukture, ključno je pitanje "upravljanja zaštitom podataka" kako bi se osigurala jasna odgovornost fizičke osobe koja predstavlja tvrtku i konkretne funkcionalne odgovornosti unutar strukture, primjerice povjeravajući druge osobe da djeluju kao predstavnici ili kontaktne točke za osobe čiji se podaci obrađuju.

Posebna analiza potrebna je u slučajevima kada fizička osoba koja djeluje u okviru pravne osobe koristi podatke za svoje potrebe izvan opsega i moguće kontrole aktivnosti pravne osobe U ovom slučaju, uključena fizička osoba bila bi kontrolor obrade o kojoj se odlučivao, te bi snosio odgovornost za tu uporabu osobnih podataka. Izvorni kontrolor ipak bi mogao zadržati određenu odgovornost u slučaju da se nova obrada dogodila zbog nedostatka odgovarajućih sigurnosnih mjera.

Kao što je već spomenuto, uloga kontrolora ključna je i posebno važna kada se radi o utvrđivanju odgovornosti i izricanju sankcija. Čak i ako se odgovornost i sankcije razlikuju ovisno o državama članicama, budući da se one nameću u skladu s nacionalnim zakonima, potreba da se jasno identificira fizička ili pravna osoba odgovorna za kršenje zakona o zaštiti podataka je nesumnjivo osnovni preduvjet za učinkovito primjene Direktive.

Identifikacija „kontrolora" u perspektivi zaštite podataka u praksi će se međusobno povezivati s građanskim, upravnim ili kaznenim pravom kojim se predviđa raspodjela odgovornosti ili sankcija kojima može biti podvrgnuta pravna ili fizička osoba[14]

Građanska odgovornost ne bi trebala pokrenuti određena pitanja u ovom kontekstu jer se ona u načelu primjenjuje na pravne i fizičke osobe. Međutim, kaznena i / ili upravna odgovornost može se prema nacionalnom pravu ponekad odnositi samo na fizičke osobe. Ako postoje kaznene ili administrativne sankcije za povrede zaštite podataka u skladu s odgovarajućim nacionalnim zakonom, ovaj zakon će normalno također odlučiti tko je odgovoran: u slučajevima kada se ne priznaje kaznena ili upravna odgovornost pravnih osoba, takvu odgovornost mogu preuzeti funkcioneri pravnih osoba prema posebnim pravilima nacionalnog prava[15]

---

13 Slično obrazloženje primjenjuje se u odnosu na Uredbu (EZ) br. U praksi supervizije jasno je istaknuto da dužnosnici institucija i tijela EU-a, koji su imenovani kao „kontrolori", djeluju u ime tijela za koje rade.

14 Vidi Komisijsku "Usporednu studiju o situaciji u 27 država članica u vezi s pravom primjenjivim na izvanugovorne obveze koje proizlaze iz kršenja privatnosti i prava u vezi s osobnošću", veljača 2009., dostupno na http://ec.europa.eu/justice_home/doc_centre/civil/studies/doc/study_privacy_en.pdf

15 To ne isključuje da nacionalni zakoni mogu predvidjeti kaznenu ili upravnu odgovornost ne samo za kontrolora, već i za svaku osobu koja krši zakon o zaštiti podataka.

Europsko pravo sadrži korisne primjere kriterija kojima se pripisuje kaznena odgovornost[16], osobito kada je kazneno djelo počinjeno u korist pravne osobe: Odgovornost se u tom slučaju može pripisati bilo kojoj osobi, "koja djeluje pojedinačno ili kao dio organa pravne osobe koja ima vodeću poziciju u pravnoj osobi, na temelju jednog od sljedećih:
(a) ovlasti za zastupanje pravne osobe;
(b) ovlasti za donošenje odluka u ime pravne osobe;
(c) ovlasti za obavljanje kontrole unutar pravne osobe. "

Preliminarni zaključak

Sumirajući gore navedena razmišljanja, može se zaključiti da je odgovoran za kršenje zaštite podataka uvijek kontrolor, tj. Pravna osoba (tvrtka ili javno tijelo) ili fizička osoba koja je formalno identificirana prema kriterijima Direktive. Ako fizička osoba koja radi u poduzeću ili javnom tijelu koristi podatke u svoje svrhe, izvan djelatnosti tvrtke, ta se osoba smatra de facto upraviteljem i odgovorna je kao takva.

Primjer br. 4: Tajno praćenje zaposlenika

Član uprave tvrtke odluči tajno pratiti zaposlenike tvrtke
tvrtke, iako ta odluka formalno nije odobrena od strane uprave.
treba smatrati kontrolorom i suočiti se s mogućim potraživanjima i obvezama
u odnosu na zaposlenike čiji su osobni podaci zloupotrijebljeni.

Odgovornost tvrtke je osobito zbog činjenice da kao kontrolor ima
obvezu osiguranja poštivanja pravila o sigurnosti i povjerljivosti. Zlouporaba od strane
funkcioner tvrtke ili zaposlenik može se smatrati kao rezultat toga
neprikladne sigurnosne mjere. To je bez obzira na to je li u kasnijoj fazi i
član uprave ili druge fizičke osobe u društvu
iz građanskopravne perspektive - i prema poduzeću - kao i iz tvrtke
perspektiva kaznenog prava. To bi mogao biti slučaj npr. Ako je član uprave koristio
prikupljeni podaci za iznudu osobnih usluga od zaposlenika: on bi morao biti
smatraju se kontrolorima i odgovorni su za tu specifičnu uporabu podataka.

III.1.d) Drugi element: "sam ili zajedno s drugima"

Ovaj će se stavak, oslanjajući se na prethodnu analizu tipičnih karakteristika kontrolora, baviti onim slučajevima u kojima više sudionika sudjeluje u obradi osobnih podataka. Doista, sve je veći broj slučajeva u kojima različiti akteri djeluju kao kontrolori, a definicija iz Direktive usmjerena je na to.

Mogućnost da upravitelj djeluje "sam ili zajedno s drugima" nije spomenuta u Konvenciji 108 i zapravo ju je uveo samo Europski parlament prije usvajanja Direktive. U mišljenju Komisije o EP-u

[16] Vidi npr. Direktivu 2008/99 / EZ od 19. studenoga 2008. o zaštiti okoliša kroz kazneno pravo, Okvirnu odluku Vijeća od 13. lipnja 2002. o borbi protiv terorizma. Pravni instrumenti temelje se na članku 29., članku 31. točki (e) i članku 34. stavku 2. točki (b) UEU-a ili odgovaraju pravnim temeljima za instrumente koji se koriste u prvom stupu, a koji proizlaze iz sudske prakse Europskog suda pravde u predmetima C-176/03 , COM / Vijeće, [ECJR] 2005, I-7879 i C-440/05, COM / Vijeće, [ECJR] 2007, I-9097. Vidi također Komunikaciju COM (2005) 583 final.

izmjene i dopune, Komisija upućuje na mogućnost da*za jedan postupak obrade određeni broj stranaka može zajednički odrediti svrha i sredstva obrade koja će se izvršiti "i stoga da se u takvom slučaju" svaki od kontrolera mora smatrati ograničenim obvezama koje nameće Direktiva kako bi se zaštitile fizičke osobe o kojima se obrađuju podaci*".

Mišljenje Komisije nije u potpunosti odrazilo složenost trenutne stvarnosti obrade podataka, budući da se usredotočila samo na slučaj gdje svi kontrolori jednako određuju i jednako su odgovorni za jedan postupak obrade. Umjesto toga, stvarnost pokazuje da je to samo jedna od različitih vrsta 'pluralističke kontrole' koja može postojati. U toj perspektivi, "zajednički" se mora tumačiti kao značenje "zajedno s" ili "ne samo" u različitim oblicima i kombinacijama.

Prije svega, treba napomenuti da je vjerojatnost više sudionika u obradi osobnih podataka prirodno povezana s više vrsta aktivnosti koje prema Direktivi mogu biti "obrada", koja je na kraju dana predmet "zajedničke kontrole". Definicija obrade iz članka 2.b Direktive ne isključuje mogućnost da različiti sudionici sudjeluju u različitim operacijama ili skupovima operacija na osobnim podacima. Te se operacije mogu odvijati istovremeno ili u različitim fazama.

U tako složenom okruženju jest još je važnije da se uloge i odgovornosti mogu lako dodijeliti, kako bi se osiguralo da složenost zajedničke kontrole ne rezultira neupotrebljivom raspodjelom odgovornosti koja bi ugrozila učinkovitost zakona o zaštiti podataka. Nažalost, zbog mnogostrukosti mogućih aranžmana, nije moguće izraditi iscrpan "zatvoreni" popis ili kategorizaciju različitih vrsta "zajedničke kontrole". Međutim, korisno je u ovom kontekstu dati i upute kroz neke kategorije i primjere zajedničke kontrole te kroz neke činjenične elemente iz kojih se može zaključiti ili pretpostaviti zajednička kontrola.

Općenito, procjena zajedničke kontrole trebala bi odražavati ocjenu "jedinstvene" kontrole koja je razvijena gore u stavku III.1.a do c. U istoj liniji, također u procjeni zajedničke kontrole treba uzeti suštinski i funkcionalni pristup, kao što je gore prikazano, usredotočujući se na to da li svrhe i sredstva određuje više od jedne strane.

Primjer br. 5: Instaliranje kamera za video nadzor

Vlasnik zgrade sklapa ugovor s osiguravajućim društvom, tako da on u ime kontrolora instalira neke kamere u različitim dijelovima zgrade. Svrhe videonadzora i način na koji se slike prikupljaju i pohranjuju određuje isključivo vlasnik zgrade, te se stoga mora smatrati isključivim upravljačem za ovu obradu.

Također, u ovom kontekstu, ugovorni aranžmani mogu biti korisni u procjeni zajedničke kontrole, ali uvijek se moraju provjeriti u odnosu na činjenične okolnosti odnosa između stranaka.

Primjer br. 6: headhunters

Tvrtka Headhunterz Ltd pomaže Enterprize Inc u zapošljavanju novih djelatnika. Ugovor jasno navodi da će "Headhunterz Ltd" djelovati u ime Enterprize i u obradi osobni podaci djeluju kao obrađivači podataka. Enterprize je jedini kontrolor podataka ". Međutim, Headhunterz doo je u dvosmislenom položaju: s jedne strane igra ulogu kontroler prema tražiteljima zaposlenja, s druge strane pretpostavlja da je procesor djeluje u ime kontrolora, kao što su Enterprize Inc i druge tvrtke koje traže osoblje kroz njega. Nadalje, Headhunterz - sa svojim poznatim uslugama s dodanom vrijednošću - globalni matchz "- traži prikladne kandidate kako među životopisima koje je izravno primio Enterprize i one koje već ima u svojoj opsežnoj bazi podataka. To osigurava da Headhunterz, koji se prema ugovoru plaća samo za ugovore koji su zapravo potpisani, povećava usklađenost između ponuda za posao i tražitelja zaposlenja, čime se povećavaju njegovi prihodi. Iz gore navedenih elemenata može se reći da, usprkos ugovornoj kvalifikaciji, Headhunterz doo će se smatrati kontrolorom i kontrolirati zajedno Enterprize Inc barem one skupine operacija koje se odnose na zapošljavanje poduzeća.

U tom pogledu, zajednička kontrola će se pojaviti kada različite strane u pogledu specifičnih operacija obrade utvrde svrhu ili one bitne elemente sredstava koji karakteriziraju kontrolora (vidi stavak III.1.a do c).

Međutim, u kontekstu zajedničke kontrole sudjelovanje stranaka na zajedničko određivanje može poprimiti različite oblike i ne mora se jednako dijeliti Doista, u slučaju pluralnosti aktera, oni mogu imati vrlo bliske odnose (dijeljenje, na primjer, svih svrha i sredstava obrade) ili labavija veza (na primjer, dijeljenje samo svrhe ili sredstva, ili njihov dio) , Stoga bi trebalo razmotriti široku paletu tipologija za zajedničku kontrolu i procijeniti njihove pravne posljedice, dopuštajući određenu fleksibilnost kako bi se osigurala sve veća složenost trenutne stvarnosti obrade podataka.

U tom kontekstu, potrebno je rješavati različite stupnjeve u kojima više strana može međusobno djelovati ili biti međusobno povezane u obradi osobnih podataka.

Prije svega, sama činjenica da različiti subjekti surađuju u obradi osobnih podataka, na primjer u lancu, ne podrazumijeva da su oni zajednički kontrolori u svim slučajevima, budući da razmjena podataka između dviju stranaka bez potrebe za dijeljenjem ili značenjem u zajedničkom skup operacija treba smatrati samo prijenosom podataka između zasebnih kontrolora.

Primjer br. 7: Putnička agencija (1) \ t

Putnička agencija šalje osobne podatke svojih klijenata zrakoplovnim tvrtkama i lancu tvrtke hoteli, s ciljem rezerviranja turističkog paketa. Zrakoplovna i zrakoplovna tvrtka hotel potvrđuje dostupnost traženih sjedala i soba. Putnička agencija izdaje putne isprave i vaučere za svoje klijente. U ovom slučaju, putovanje agencija, zrakoplovna tvrtka i hotel bit će tri različita kontrolora podataka obveze zaštite podataka koje se odnose na vlastitu obradu osobnih podataka.

Međutim, procjena se može promijeniti kada bi različiti sudionici odlučili uspostaviti zajedničku infrastrukturu kako bi ostvarili vlastite pojedinačne svrhe. Kada to postavljate

infrastruktura ti sudionici određuju bitne elemente sredstava koja će se koristiti, oni se kvalificiraju kao zajednički kontrolori podataka - u svakom slučaju u toj mjeri - čak i ako ne moraju nužno dijeliti iste svrhe.

Primjer br. 8: Putnička agencija (2) \ t

Putnička agencija, hotelski lanac i zrakoplovna tvrtka odlučuju osnovati internetsku bazu zajedničke platforme kako bi se poboljšala njihova suradnja u pogledu putovanja upravljanje rezervacijama. Oni se slažu oko važnih elemenata sredstava koja će se koristiti, kao što su podaci koji će biti pohranjeni, kako će rezervacije biti dodijeljene i potvrđene, i tko može imati pristup pohranjenim informacijama. Nadalje, odlučuju podijeliti podatke svojih kupaca kako bi mogli provesti integrirane marketinške akcije.

U ovom slučaju, putnička agencija, zrakoplovna tvrtka i lanac hotela imat će zajedničku kontrolu kako se obrađuju osobni podaci njihovih kupaca i stoga će biti zajednički kontrolori u vezi s postupcima obrade koji se odnose na zajednički internetska rezervacijska platforma. Međutim, svaki od njih bi i dalje zadržao isključivu kontrolu u odnosu na druge aktivnosti obrade, npr. one koje se odnose na upravljanje njihovim ljudski resursi.

U nekim slučajevima različiti sudionici obrađuju iste osobne podatke u nizu. U tim slučajevima, vjerojatno je da se na mikro razini različite operacije obrade lanca pojavljuju kao nepovezane, jer svaka od njih može imati različitu svrhu. Međutim, potrebno je provjeriti jesu li se na makro razini te operacije obrade ne bi trebale smatrati „skupom operacija“ koje se provode u zajedničkoj svrsi ili korištenjem zajednički definiranih sredstava.

Sljedeća dva primjera objašnjavaju ovu ideju davanjem dva različita scenarija.

Primjer br. 9: Prijenos podataka zaposlenika poreznim vlastima

Tvrtka XYZ prikuplja i obrađuje osobne podatke svojih zaposlenika sa svrhom upravljanja plaćama, misijama, zdravstvenim osiguranjima itd. Međutim, zakon također nameće obvezu tvrtke da sve podatke o plaćama pošalje poreznim vlastima, s ciljem jačanja fiskalne kontrole.

U ovom slučaju, iako obje tvrtke XYZ i porezne vlasti procesuiraju isto podaci o plaćama, nedostatak zajedničke svrhe ili sredstava u vezi s tim podacima obrada će rezultirati kvalificiranjem dva entiteta kao dva odvojena kontrolora podataka.

Primjer br. 10: Financijske transakcije

Umjesto toga, uzmimo slučaj banke koja koristi prijevoznika financijskih poruka kako bi obavljati svoje financijske transakcije. I banka i prijevoznik se slažu oko sredstava obrade financijskih podataka. Obrada osobnih podataka koji se odnose financijske transakcije provodi u prvoj fazi samo financijska institucija u kasnijoj fazi nositeljem financijskih poruka. Međutim, čak i na mikro razini od tih subjekata slijedi svoju svrhu, na makro razini različite faze i svrhe i sredstva obrade usko su povezani. U ovom slučaju, obje banke i nosač poruke može se smatrati zajedničkim kontrolorima.

Postoje i drugi slučajevi u kojima različiti uključeni sudionici zajednički određuju, u nekim slučajevima u različitoj mjeri, svrhe i / ili sredstva operacije obrade.

Postoje slučajevi u kojima je svaki kontrolor odgovoran samo za dio obrade, ali informacije se sastavljaju i obrađuju putem platforme.

Primjer br. 11: Portali e-uprave

Portali e-uprave djeluju kao posrednici između građana i javnosti jedinice uprave: portal prenosi zahtjeve građana i depozite dokumente jedinice javne uprave dok ih građanin ne opozove. Svaki Jedinica javne uprave ostaje kontrolor podataka koji se obrađuju za vlastite svrhe. Unatoč tome, sam portal može se također smatrati kontrolorom. Doista, to postupke (tj. prikuplja i prenosi nadležnoj jedinici) zahtjeve građana kao i javne dokumente (tj. pohranjuje ih i regulira svaki njihov pristup, npr građanima) za daljnje svrhe (olakšavanje e-uprave usluge) od onih za koje su podaci u početku obrađeni u svakoj javnosti jedinica uprave. Ti će kontrolori, među ostalim obvezama, to osigurati sustav za prijenos osobnih podataka od korisnika u sustav javne uprave je siguran, jer je na makro razini taj prijenos bitan dio skupa obrade operacije koje se provode putem portala.

Druga moguća struktura je "pristup temeljen na podrijetlu", koji nastaje kada je svaki kontrolor odgovoran za podatke koje uvodi u sustav. To je slučaj s nekim bazama podataka na razini EU-a, gdje se kontrola - a time i obveza postupanja po zahtjevima za pristup i ispravak - pripisuje na temelju nacionalnog podrijetla osobnih podataka.

Još jedan zanimljiv scenarij nude online društvene mreže.

Primjer br. 12: Društvene mreže

Pružatelji usluga društvenih mreža pružaju mrežne komunikacijske platforme koje pojedincima omogućuju objavljivanje i razmjenu informacija s drugim korisnicima. Ovi pružatelji usluga su kontrolori podataka, budući da određuju i svrhu i način obrade takvih informacija. Korisnici takvih mreža, učitavajući osobne podatke i trećih osoba, smatrali bi se kontrolorima pod uvjetom da njihove aktivnosti ne podliježu tzv. [17]

Nakon analize onih slučajeva u kojima različiti subjekti zajednički određuju samo dio svrhe i sredstva, vrlo jasan i neproblematični slučaj je onaj u kojem više subjekata zajednički određuje i dijeli sve svrhe i sredstva obrade aktivnosti, što dovodi do potpunog zajednička kontrola.

[17] Za više detalja i primjere, vidi Mišljenje 5/2009 Radne skupine o internetskim društvenim mrežama, usvojeno 12. lipnja 2009. (WP 163)

U potonjem slučaju, lako je utvrditi tko je nadležan i koji je u stanju osigurati prava subjekata podataka, kao i poštivati obveze zaštite podataka. Međutim, zadaća određivanja nadležnog i odgovornog kontrolora za koja su prava i obveze nositelja podataka mnogo složenija kada različite upravitelje dijele ciljeve i sredstva obrade na asimetričan način.

Potrebno je razjasniti raspodjelu kontrole

Prije svega, treba naglasiti da, posebno u slučajevima zajedničke kontrole, nemogućnost izravnog ispunjavanja svih obveza kontrolora (osiguravanje informacija, pravo pristupa, itd.) Ne isključuje mogućnost kontrole. Moguće je da bi u praksi te obveze mogle lako ispuniti druge stranke, koje su ponekad bliže subjektu podataka, u ime kontrolora. Međutim, kontrolor će u svakom slučaju ostati odgovoran za svoje obveze i odgovoran za bilo kakvo kršenje istih.

Prema prethodnom tekstu koji je Komisija predstavila tijekom procesa donošenja Direktive, pristup određenim osobnim podacima podrazumijevao bi (zajednički) kontrolor tih podataka. Međutim, ova formulacija nije zadržana u konačnom tekstu, a iskustvo pokazuje da pristup podacima s jedne strane ne podrazumijeva takvu kontrolu, dok s druge strane pristup podacima nije bitan uvjet za kontrolora. Stoga u složenim sustavima s višestrukim akterima pristup osobnim podacima i drugim subjektima podataka može biti osiguran na različitim razinama od strane različitih sudionika.

Pravne posljedice odnose se i na odgovornost kontrolora, posebno u vezi s pitanjem da li „zajednička kontrola“ uspostavljena Direktivom uvijek podrazumijeva solidarnu odgovornost. Onlanak 26. o odgovornosti koristi jedninu „kontrolor“, što ukazuje na pozitivan odgovor. Međutim, kao što je već spomenuto, stvarnost može predstaviti različite načine djelovanja „zajedno“, tj. „Zajedno s“. To bi u nekim okolnostima moglo dovesti do solidarne odgovornosti, ali ne u pravilu: u mnogim slučajevima različiti kontrolori mogu biti odgovorni - i stoga odgovorni - za obradu osobnih podataka u različitim fazama i različitim stupnjevima.

Zaključak bi trebao biti da čak iu složenim okruženjima za obradu podataka, gdje različiti kontroleri igraju ulogu u obradi osobnih podataka, poštivanje pravila o zaštiti podataka i odgovornosti za moguće kršenje ovih pravila su jasno dodijeljena, kako bi se izbjeglo smanjenje zaštite osobnih podataka ili da dođe do "negativnog sukoba kompetencija" i rupa u zakonu, neke od stranaka ne osiguravaju neke obveze ili prava koje proizlaze iz Direktive.

U tim slučajevima, više nego ikad, važno je dati subjektima podataka jasnu informativnu obavijest, objašnjavajući različite faze i aktere obrade. Štoviše, treba biti jasno da li je svaki kontrolor nadležan za poštivanje prava svih subjekata podataka ili koji je nadležan za koje pravo.

Primjer br. 13: Banke i baze podataka o klijentima koji ne ispunjavaju obveze

Nekoliko banaka može uspostaviti zajedničku „bazu podataka“ - gdje to dopušta nacionalno pravo za te skupine - pri čemu svaki od njih doprinosi informacijama (podacima) klijenti koji ne ispunjavaju obveze i svi oni imaju pristup ukupnoj količini informacija. Neka zakonodavstva predviđaju da svi zahtjevi subjekata podataka, npr. Za pristup ili brisanje, potrebno je napraviti samo na jednoj “ulaznoj točki”, davatelju usluga. Za to je odgovoran davatelj usluga pronalaženje odgovarajućeg kontrolera i organiziranje odgovarajućih odgovora na podatke predmet. Identitet pružatelja usluga objavljuje se u Registru obrade podataka. U takvim skupinama informacija mogu upravljati odvojeni pravni subjekti kao kontroler, dok zahtjeve za pristup subjektu obavljaju banke sudionice kao posrednik.

Primjer br. 14: Bihevioralno oglašavanje

Bihevioralno oglašavanje upotrebljava prikupljene podatke o ponašanju pojedinca za pregledavanje weba, kao što su posjećene stranice ili izvršena pretraživanja, kako bi odabrala oglase za prikazivanje tom pojedincu. Oba izdavača, koji vrlo često iznajmljuju prostore za oglašavanje na svojim web-lokacijama i pružatelje oglasnih mreža, koji popunjavaju te prostore ciljanim oglašavanjem, mogu prikupljati i razmjenjivati informacije o korisnicima, ovisno o određenim ugovornim uvjetima.

Iz perspektive zaštite podataka, izdavač se smatra autonomnim kontrolorom u onoj mjeri u kojoj prikuplja osobne podatke od korisnika (korisnički profil, IP adresu, lokaciju, jezik operativnog sustava itd.) Za vlastite potrebe. Davatelj oglasne mreže također će biti kontrolor u onoj mjeri u kojoj određuje svrhe (praćenje korisnika na web-lokacijama) ili osnovna sredstva obrade podataka. Ovisno o uvjetima suradnje između izdavača i pružatelja oglasne mreže, na primjer ako izdavač omogućuje prijenos osobnih podataka pružatelju oglasne mreže, uključujući, primjerice, preusmjeravanje korisnika na web-stranicu oglasne mreže mogu biti zajednički kontrolori za skup postupaka obrade koji dovode do oglašavanja ponašanja.

U svim slučajevima, (zajednički) kontrolori moraju osigurati da složenost i tehničke značajke sustava oglašavanja ponašanja ne sprječavaju njih u pronalaženju odgovarajućih načina usklađivanja s obvezama kontrolora i osiguravanjem prava osoba na koje se podaci odnose. To bi osobito uključivalo:

- *informacija* da korisnik ima pristup podacima treće strane: to bi mogao biti učinkovitiji od strane izdavača koji je glavni sugovornik korisnika,

- i uvjeti *pristup* na osobne podatke: tvrtka za oglasne mreže trebala bi odgovoriti na zahtjeve korisnika o načinu na koji obavljaju ciljano oglašavanje na podacima korisnika te se pridržavati zahtjeva za ispravljanje i brisanje.

Osim toga, izdavači i davatelji oglasnih mreža mogu podlijegati drugim obvezama koje proizlaze iz zakona o građanskim pravima i zaštiti potrošača, uključujući zakone o oduzimanju prava i nepoštene poslovne prakse.

Preliminarni zaključak

Stranke koje djeluju zajednički imaju određeni stupanj fleksibilnosti u raspodjeli i raspodjeli obveza i odgovornosti među njima, sve dok osiguravaju potpunu usklađenost. Pravila o tome kako izvršavati zajedničke odgovornosti trebaju u načelu odrediti kontrolori. Međutim, u ovom slučaju treba razmotriti činjenične okolnosti kako bi se procijenilo da li aranžmani odražavaju stvarnost obrade temeljnih podataka.

U tom pogledu, procjena zajedničke kontrole trebala bi uzeti u obzir, s jedne strane, potrebu da se osigura potpuna usklađenost s pravilima o zaštiti podataka, as druge strane da umnožavanje kontrolora može također dovesti do neželjenih složenosti i mogućeg nedostatka jasnoća u raspodjeli odgovornosti. To bi dovelo do nezakonitosti cjelokupne obrade zbog nedostatka transparentnosti i kršenja načela poštene obrade.

Primjer br. 15: Platforme za upravljanje zdravstvenim podacima

U državi članici, javna vlast uspostavlja nacionalnu točku prijelaza koja regulira. \ T razmjenu podataka o pacijentima između pružatelja zdravstvenih usluga. Veći broj kontrolera - desetine tisuća - rezultira u tako nejasnoj situaciji za osobe čiji se podaci obrađuju (pacijenti) da bi zaštita njihovih prava bila u opasnosti. Doista, za osobe čiji se podaci obrađuju biti nejasni kome bi se mogli obratiti u slučaju pritužbi, pitanja i zahtjeva za informacije, ispravke ili pristup osobnim podacima. Nadalje, javna vlast je odgovorni za stvarni dizajn obrade i način na koji se ona koristi. To elementi dovode do zaključka da je javno tijelo utvrdilo mjesto prebacivanja smatraju se zajedničkim kontrolorom, kao i kontaktnom točkom za osobe čiji se podaci obrađuju zahtjevi.

U tom kontekstu, može se tvrditi da se solidarna odgovornost za sve uključene strane treba smatrati sredstvom za uklanjanje neizvjesnosti, te se stoga pretpostavlja samo u onoj mjeri u kojoj nije postojala alternativna, jasna i jednako učinkovita raspodjela obveza i odgovornosti. utvrđene od strane uključenih strana ili ne proizlaze jasno iz činjeničnih okolnosti.

III.2. Definicija procesora

Koncept procesora nije utvrđen Konvencijom 108. Prvi put je uloga procesora prepoznata u prvom prijedlogu Komisije, ali bez uvođenja ovog koncepta, s ciljem da se "*izbjegavati situacije u kojima obrada od strane treće strane u ime kontrolora spisa ima za posljedicu smanjenje razine zaštite koju uživa subjekt podataka*". Samo s izmijenjenim prijedlogom Komisije i na prijedlog Europskog parlamenta, pojam procesora izričito je i autonomno razrađen, prije nego što se trenutna formulacija u Zajedničkom stajalištu Vijeća usvoji.

Na isti način kao i za definiciju kontrolora, definicija procesora predviđa širok raspon sudionika koji mogu igrati ulogu procesora („... fizičke ili pravne osobe, javne vlasti, agencije ili bilo kojeg drugog tijela ... „).

Postojanje procesora ovisi o odluci kontrolora, koja može odlučiti da li će obraditi podatke unutar svoje organizacije, primjerice putem osoblja ovlaštenog za obradu podataka pod njegovim izravnim ovlastima (vidi *a contrario* Članak 2.f), ili delegirati sve ili dio aktivnosti obrade na vanjsku organizaciju, tj. - kao što je navedeno u obrazloženju izmijenjenog prijedloga Komisije - od "pravno odvojene osobe koja djeluje u njegovo ime".

Stoga su, s jedne strane, dva osnovna uvjeta za kvalifikaciju kao procesor a zasebna pravna osoba u odnosu na kontrolora as druge strane obrade osobnih podataka u njegovo ime Ova aktivnost obrade može biti ograničena na vrlo specifičan zadatak ili kontekst ili može biti općenitija i proširena.

Nadalje, uloga procesora ne proizlazi iz prirode entiteta koji obrađuje podatke, nego iz njegove konkretne aktivnosti u određenom kontekstu Drugim riječima, isti subjekt može djelovati istovremeno kao kontrolor za određene operacije obrade i kao procesor za druge, a kvalifikacija kontrolora ili procesora mora se procijeniti s obzirom na određene skupove podataka ili operacija.

Primjer br. 16: Davatelji internetskih usluga hosting usluga

ISP koji pruža usluge hostinga je u načelu procesor osobnih podataka objavili online od strane svojih kupaca, koji koriste ovaj ISP za svoje web hosting i održavanje. Međutim, ako ISP dodatno obrađuje podatke za svoje potrebe sadržane na web-stranicama, onda je to kontrolor podataka s obzirom na to specifično obrada. Ova se analiza razlikuje od ISP-a koji pruža e-poštu ili pristup internetu usluge (vidi također primjer br. 1: telekom operateri).

Najvažniji element je propis koji procesor djeluje "...u ime kontrolora...". Djelovati u ime znači služiti tuđem interesu i podsjeća na pravni pojam "delegacije". U slučaju zakona o zaštiti podataka, obrađivač je pozvan provesti upute koje je dao kontrolor barem s obzirom na svrhu obrade i bitne elemente sredstava.

U tom pogledu, zakonitost aktivnosti obrade podataka procesora određena je ovlaštenjem koje je dao kontrolor. Procesor koji prelazi svoj mandat i dobiva važnu ulogu u određivanju svrhe ili osnovnog načina obrade je (zajednički) kontrolor, a ne procesor. Pitanje zakonitosti ove obrade i dalje će se ocjenjivati u svjetlu drugih članaka (6-8). Međutim, delegiranje još uvijek može podrazumijevati određeni stupanj diskrecije o tome kako najbolje služiti interesima kontrolora, dopuštajući obrađivaču da odabere najprikladnija tehnička i organizacijska sredstva.

Primjer br. 17: Outsourcing poštanskih usluga

Privatna tijela pružaju poštanske usluge u ime (javnih) agencija - npr obiteljske i rodiljne naknade izvršene u ime Nacionalnog socijalnog osiguranja Agencija. U tom slučaju DPA je navela da bi privatna tijela trebala biti imenovan kao prerađivač s obzirom da je njihov zadatak, premda se obavlja s određenim stupnja autonomije, bio je ograničen samo na dio potrebnih operacija obrade za svrhe koje je odredio kontrolor podataka.

Ipak, kako bi se osiguralo da outsourcing i delegiranje ne rezultiraju smanjenjem standarda zaštite podataka, Direktiva sadrži dvije odredbe koje su posebno upućene obrađivaču i koje detaljno definiraju njegove obveze u pogledu povjerljivosti i sigurnosti.

- Člankom 16. utvrđuje se da ih sam obrađivač, kao i svaka osoba koja djeluje pod njegovim ovlastima, a ima pristup osobnim podacima, ne smije obraditi, osim prema uputama kontrolora.

- Članak 17. u odnosu na sigurnost obrade utvrđuje potrebu za ugovorom ili obvezujućim pravnim aktom kojim se uređuju odnosi između kontrolora podataka i obrađivača podataka. Ovaj ugovor mora biti u pisanoj formi radi dokazivanja i mora sadržavati minimalni sadržaj, posebno propisujući da obrađivač podataka djeluje samo po uputama kontrolora i provodi tehničke i organizacijske mjere za adekvatnu zaštitu osobnih podataka. Ugovor bi trebao sadržavati dovoljno detaljan opis mandata obrađivača.

S tim u vezi, treba napomenuti da će pružatelji usluga specijalizirani za određenu obradu podataka (na primjer, isplata plaća) u mnogim slučajevima uspostaviti standardne usluge i ugovore koje će potpisati kontrolori podataka, te će de facto odrediti određeni standardni način obrade osobnih podataka[18] Međutim, činjenica da ugovor i njegovi detaljni uvjeti poslovanja priprema davatelj usluga, a ne kontrolor nije *u sebi* dovoljna osnova za zaključak da bi se pružatelj usluga trebao smatrati kontrolorom, u mjeri u kojoj je kontrolor slobodno prihvatio ugovorne uvjete, prihvaćajući na taj način punu odgovornost za njih.

U istom smislu, neravnoteža ugovorne ovlasti malog kontrolora podataka u odnosu na velike pružatelje usluga ne bi se trebala smatrati opravdanjem za kontrolora da prihvati klauzule i uvjete ugovora koji nisu u skladu sa zakonom o zaštiti podataka.

Primjer br. 18: Platforme za e-poštu

John Smith traži platformu za e-poštu koju će koristiti sam i pet zaposlenika njegove tvrtke. On otkriva da je prikladna platforma pogodna za korisnika - i također jedina jedan besplatan - čuva osobne podatke za prekomjerno vrijeme i prijenos trećim zemljama bez odgovarajućih mjera zaštite. Nadalje, ugovorni pojmovi su "uzmi ili ostavi".

U ovom slučaju, g. Smith bi trebao tražiti drugog pružatelja usluga ili - u slučaju navodnog nepridržavanje pravila o zaštiti podataka ili nedostatak dostupnosti na tržištu drugih odgovarajuće davatelje - uputite slučaj nadležnim tijelima, kao što su DPA, potrošači antimonopolske vlasti, itd.

Činjenica da Direktiva zahtijeva pisani ugovor kako bi se osigurala sigurnost obrade ne znači da ne mogu postojati odnosi kontrolora / procesora bez prethodnih ugovora. U tom smislu, ugovor nije ni konstitutivan ni odlučujući, čak i ako je riječ o ugovoru

[18] Razrada uvjeta ugovora od strane pružatelja usluga ne dovodi u pitanje činjenicu da kontrolor određuje bitne aspekte obrade, kako je opisano u točki III.1.b.

može pomoći u boljem razumijevanju odnosa između stranaka[19] Stoga će se iu ovom slučaju primijeniti funkcionalni pristup, analizirajući činjenične elemente odnosa između različitih subjekata i način određivanja svrhe i načina obrade. U slučaju postojanja odnosa upravitelja / procesora, te su stranke obvezne sklopiti ugovor u skladu sa zakonom (vidi članak 17. Direktive).

Mnoštvo procesora

Sve se više događa da se obrada osobnih podataka vrši od strane kontrolora na nekoliko procesora podataka. Ti prerađivači mogu imati izravan odnos s kontrolorom podataka ili biti podizvođači kojima su prerađivači delegirali dio aktivnosti obrade koje su im povjerene.

Te složene (višestupanjske ili difuzne) strukture obrade osobnih podataka povećavaju se s novim tehnologijama, a neki nacionalni zakoni izričito se pozivaju na njih. Ništa u Direktivi ne sprječava da se zbog organizacijskih zahtjeva više subjekata može odrediti kao obrađivač podataka ili (pod) procesor tako da se podijele relevantni zadaci. Međutim, svi oni moraju se pridržavati uputa koje je dao kontrolor podataka u obavljanju obrade.

Primjer br. 19: Računalne mreže

Velike istraživačke infrastrukture sve više koriste distribuirano računalstvo postrojenja, posebice mreže, kako bi profitirala u smislu računalnog i skladišnog kapaciteta. rešetke instalirane u različitim istraživačkim infrastrukturama uspostavljenim u različitim zemljama. Europska mreža može se, na primjer, sastojati od nacionalnih mreža, koje su pak pod nacionalnom mrežom odgovornost nacionalnog tijela. Međutim, ova europska mreža možda neće imati središnju mrežu tijelo, odgovorno za njegovo funkcioniranje. Istraživači koji koriste takvu mrežu obično ne mogu identificirati gdje se njihovi podaci točno obrađuju, a time i tko je odgovoran procesor podataka (slučaj je još složeniji ako postoje mrežne infrastrukture u trećim zemljama). Treba li mrežna infrastruktura koristiti podatke na neovlašten način, ta se stranka može smatrati kontrolorom podataka, ako ne djeluje u ime korisnika istraživači.

Strateško pitanje ovdje je da - s mnoštvom aktera uključenih u proces - obveze i odgovornosti koje proizlaze iz zakonodavstva o zaštiti podataka i ne raspršena duž lanca outsourcinga / podugovaranja. Drugim riječima, treba izbjegavati lanac (pod) procesora koji bi razvodnio ili čak spriječio djelotvornu kontrolu i jasnu odgovornost za aktivnosti obrade, osim ako su odgovornosti različitih strana u lancu jasno utvrđene.

U toj perspektivi, u istoj liniji kao što je opisano gore u stavku III.1.b - iako nije potrebno da kontrolor definira i suglasi se o svim pojedinostima o sredstvima koja se koriste za ostvarenje predviđenih svrha - ipak bi bilo potrebno barem je informiran o glavnim elementima obradne strukture (na primjer, uključeni subjekti, sigurnost

[19] Međutim, u nekim slučajevima postojanje pisanog ugovora može predstavljati nužan uvjet za automatsko kvalificiranje kao procesor u određenim kontekstima. U Španjolskoj, primjerice, izvješće o pozivnim centrima definira kao procesore sve pozivne centre u trećim zemljama, sve dok se pridržavaju ugovora. To je slučaj čak i ako je ugovor izrađen od strane procesora i kontrolor se samo "pridržava" s njim.

mjere, jamstva za obradu u trećim zemljama itd.), tako da on još uvijek može kontrolirati podatke koji se obrađuju u njegovo ime.

Također se smatra da, iako Direktiva nameće odgovornost kontroloru, ona ne sprječava nacionalne zakone o zaštiti podataka da, osim toga, i procesor treba smatrati odgovornim u određenim slučajevima.

Neki kriteriji mogu biti korisni u određivanju kvalifikacije različitih uključenih subjekata:

- Razina prethodnih uputa koje daje kontrolor podataka, koja određuje granicu manevra koju je ostavio obrađivač podataka;

- Nadzor od strane kontrolora podataka o izvršenju usluge. Kontinuirani i pažljivi nadzor od strane kontrolora kako bi se osigurala temeljita usklađenost procesora s uputama i uvjetima ugovora, ukazuje na to da je kontrolor još uvijek u potpunoj i isključivoj kontroli postupaka obrade;

- Vidljivost / slika koju kontrolor daje subjektu podataka i očekivanja subjekata podataka na temelju te vidljivosti.

Primjer br. 20: Pozivni centri

Kontrolor podataka preuzima neke od svojih operacija u pozivni centar i upućuje poziv da se predstavi pomoću identiteta kontrolora podataka kada poziva podatke kontrolera. U ovom slučaju očekivanja klijenata i način na koji Kontrolor se njima predstavlja putem outsourcinga tvrtke vodi do zaključak da outsourcing tvrtka djeluje kao procesor podataka za (u ime) kontroler.

- Stručnost stranaka: u određenim slučajevima, tradicionalna uloga i profesionalna stručnost pružatelja usluga imaju dominantnu ulogu, što može podrazumijevati njegovu kvalifikaciju kontrolora podataka.

Primjer br. 21: odvjetnici

Odvjetnik zastupa svog klijenta na sudu, au odnosu na ovu misiju, procese osobne podatke koji se odnose na klijentov slučaj. Pravna osnova za korištenje potrebne informacije je mandat klijenta. Međutim, ovaj mandat nije usredotočen obradu podataka, ali o zastupanju na sudu, za koju djelatnost takva zanimanja imaju tradicionalno vlastitu pravnu osnovu. Takve se profesije stoga smatraju neovisni 'kontrolori' prilikom obrade podataka tijekom pravnog zastupanja svojim klijentima.

U drugom kontekstu, bliža procjena sredstava koja se postavljaju za postizanje ciljeva također može biti odlučujuća.

Primjer br. 22: Web-lokacija "Izgubljeno i pronađeno"

Web-mjesto "izgubljeno i pronađeno" predstavljeno je kao samo procesor kakav bi bio oni koji objavljuju izgubljene predmete koji će odrediti sadržaj, a time i na mikro razini, svrhu (npr. pronalaženje izgubljenog broška, papiga itd.). Tijelo za zaštitu podataka je odbijeno ovaj argument. Web-lokacija je postavljena za poslovnu svrhu zarađivanja novca dopuštanje knjiženja izgubljenih predmeta i činjenice da nisu utvrdili koje određene stavke nisu objavljene (za razliku od određivanja kategorija stavki) kao što je definicija "kontrolora podataka" izričito ne uključuje određivanje sadržaja. Web stranica određuje uvjete postavljanja i sl odgovoran za ispravnost sadržaja.

Iako je moglo postojati tendencija da se outsourcing općenito identificira kao zadatak procesora, danas su situacije i procjene često mnogo složenije.

Primjer br. 23: računovođa

Kvalifikacija računovođa može varirati ovisno o kontekstu. Gdje računovođe pružaju usluge široj javnosti i malim trgovcima na temelju vrlo općenitog uputama ("Pripremite moje porezne prijave"), a zatim - kao što i odvjetnici djeluju slično okolnosti i iz sličnih razloga - računovođa će biti kontrolor podataka. Međutim, gdje je knjigovođa zaposlena u tvrtki i koja je detaljno opisana uputama internog računovođe, možda da izvrši detaljnu reviziju, zatim u Općenito, ako ne redoviti zaposlenik, on će biti procesor, zbog jasnoće i ograničen prostor za diskreciju. Međutim, to je podložno jedan glavni razlog, naime, ondje gdje smatraju da su otkrili zlouporabu koje su dužni prijaviti, zbog profesionalnih obveza koje duguju djeluju samostalno kao kontrolori.

Ponekad složenost operacija obrade može dovesti do toga da se više usredotoči na margine onih kojima je povjerena obrada osobnih podataka, npr. Kada obrada podrazumijeva određeni rizik privatnosti. Uvođenje novih načina obrade može dovesti do favoriziranja kvalifikacije kao kontrolora podataka, a ne kao procesora podataka. Ovi slučajevi mogu također dovesti do pojašnjenja - i imenovanja kontrolora - izričito propisanog zakonom.

Primjer br. 24: Obrada za povijesne, znanstvene i statističke svrhe

Nacionalno pravo može uvesti u pogledu obrade osobnih podataka za povijesne, znanstvene i statističke svrhe, pojam posredničke organizacije za određivanje tijelo zaduženo za pretvaranje ne-kodiranih podataka u kodirane podatke, tako da kontrolor obrade u povijesne, znanstvene i statističke svrhe
biti u mogućnosti ponovno identificirati ispitanike.

Ako više kontrolera operacija početne obrade prenosi podatke na jednu ili više trećina stranke za daljnju obradu u povijesne, znanstvene i statističke svrhe, podatke prvo kodira posrednička organizacija. U ovom slučaju posrednik organizacija može se smatrati kontrolorom u skladu s posebnim nacionalnim propisima, i podliježe svim rezultirajućim obvezama (relevantnost podataka, informiranje podataka predmet, obavijest itd.). To je opravdano činjenicom da kada se podaci razlikuju izvori prikupljeni zajedno, postoji posebna prijetnja zaštiti podataka, što opravdava vlastitu odgovornost posredničke organizacije. Prema tome, to nije jednostavno smatra se obrađivačem, ali se u potpunosti smatra kontrolorom u skladu s nacionalnim pravom.

U istom smislu, relevantna je i autonomna moć odlučivanja koja je ostavljena različitim stranama uključenim u procesiranje. Slučaj kliničkih ispitivanja lijekova pokazuje da odnos između sponzorskih tvrtki i vanjskih subjekata kojima je povjereno provođenje ispitivanja ovisi o diskreciji koja je ostavljena vanjskim subjektima u pogledu obrade podataka. To podrazumijeva da može postojati više od jednog kontrolora, ali i više procesora ili osoba zaduženih za obradu.

Primjer br. 25: Klinička ispitivanja lijekova

Farmaceutska tvrtka XYZ sponzorira neke studije o lijekovima i odabire kandidata sudskim centrima procjenom odgovarajućih uvjeta i interesa; ona sastavlja suđenje protokol, pruža potrebne smjernice centrima u vezi s obradom podataka i provjerava da li centri poštuju protokol i odgovarajuće interne procedure.

Iako sponzor ne prikuplja nikakve podatke izravno, on dobiva pacijente podatke koje prikupljaju centri za ispitivanje i obrađuju te podatke na različite načine (ocjenjujući informacije sadržane u medicinskoj dokumentaciji; primanje podataka štetnih reakcije; unos tih podataka u odgovarajuću bazu podataka; obavljanjem statističkih analiza postići rezultate ispitivanja). Sudsko središte suđenje provodi samostalno - iako u poštivanje smjernica sponzora; daje obavijesti o tome bolesnika i dobiva njihov pristanak u svezi s obradom podataka koji se odnose ih; omogućuje suradnicima sponzora pristup izvornim medicinskim pacijentima dokumente za obavljanje aktivnosti praćenja; i upravlja i odgovoran je za čuvanje tih dokumenata. Prema tome, čini se da su odgovornosti preuzete pojedinih aktera.

U tom kontekstu, u ovom slučaju, i centri za ispitivanje i sponzori su važni određivanja s obzirom na način na koji se osobni podaci koji se odnose na klinička ispitivanja obrađen. U skladu s tim, mogu se smatrati zajedničkim kontrolorima podataka. Odnos Između sponzora i sudskih centara u tim se slučajevima može različito tumačiti gdje sponzor određuje svrhu i bitne elemente sredstava i. \ t istraživaču ostaje vrlo uska margina.

III.3. Definicija treće strane

Koncept "treće strane" nije utvrđen Konvencijom 108, već je izmijenjeni prijedlog Komisije uveo na temelju amandmana koji je predložio Europski parlament. U skladu s memorandumom o objašnjenjima, izmjena i dopuna izmijenjena je kako bi se pojasnilo da treće strane ne uključuju nositelja podataka, kontrolora i bilo koju osobu ovlaštenu za obradu podataka pod izravnim ovlaštenjem kontrolora ili u njegovo ime, kao što je slučaj s procesora. Ovo znači to "*osobe koje rade za drugu organizaciju, čak i ako pripada istoj grupi ili holdingu, općenito će biti treća strana*"dok s druge strane"*podružnice bankovnih računa klijenata koji se nalaze pod izravnim ovlastima njihovog sjedišta ne bi bile treće strane*".

Direktiva koristi "treću stranu" na način koji se ne razlikuje od načina na koji se ovaj koncept obično koristi u građanskom pravu, gdje je treća strana obično subjekt koji nije dio subjekta ili sporazuma. U kontekstu zaštite podataka, ovaj pojam treba tumačiti tako da se odnosi na bilo kojeg subjekta koji nema posebnu legitimnost ili odobrenje - što bi moglo potjecati, na primjer, iz njegove uloge kontrolora, procesora ili njihovih zaposlenika - u obradi osobnih podataka.

Direktiva koristi ovaj koncept u mnogim odredbama, obično s ciljem utvrđivanja zabrana, ograničenja i obveza za slučajeve u kojima osobne podatke mogu obrađivati druge stranke koje po porijeklu nisu trebale obraditi određene osobne podatke.

U tom kontekstu, može se zaključiti da bi treća strana koja prima osobne podatke - bilo zakonito ili nezakonito - u načelu bila novi kontrolor, pod uvjetom da su drugi uvjeti za kvalifikaciju te stranke kao kontrolora i primjenu zakonodavstva o zaštiti podataka. su upoznati.

Primjer br. 26: Neovlašteni pristup zaposlenika

Zaposlenik tvrtke u obavljanju svojih zadataka upoznaje osobne podatke za koje nije ovlašten imati pristup. U ovom slučaju, taj bi zaposlenik trebao biti "treća strana" u odnosu na poslodavca, sa svim posljedicama koje iz toga proizlaze i obveze u smislu zakonitosti komunikacije i obrade podataka.

IV. Zaključci

Koncept kontrolora podataka i njegova interakcija s konceptom procesora podataka imaju ključnu ulogu u primjeni Direktive 95/46 / EZ, budući da određuju tko će biti odgovoran za poštivanje pravila o zaštiti podataka, kako subjekti podataka mogu ostvariti svoja prava , što je primjenjivo nacionalno pravo i kako učinkovito djeluju tijela za zaštitu podataka.

Organizacijska diferencijacija u javnom i privatnom sektoru, razvoj ICT-a, kao i globalizacija obrade podataka, povećavaju složenost načina na koji se obrađuju osobni podaci i zahtijevaju pojašnjenja tih koncepata, kako bi se osigurala učinkovita primjena i usklađenost praksa.

Pojam kontrolor je autonomna, u smislu da bi se trebala tumačiti uglavnom u skladu sa zakonom o zaštiti podataka Zajednice i funkcionalnim, u smislu da je namijenjena raspodjeli odgovornosti tamo gdje je činjenični utjecaj, a time i na temelju činjenične, a ne formalne analize.

Definicija u Direktivi sadrži tri glavna elementa: osobni aspekt ("*fizičku ili pravnu osobu, javno tijelo, agenciju ili bilo koje drugo tijelo*") mogućnost pluralističke kontrole ("*koji sami ili zajedno s drugima*"); i bitne elemente za razlikovanje kontrolora od drugih sudionika ("*određuje svrhu i način obrade osobnih podataka*„).

Analiza ovih blokova dovodi do sljedećih glavnih ishoda:

- Sposobnost da*odrediti* svrhe i sredstva
  "mogu proizlaziti iz različitih pravnih i / ili činjeničnih okolnosti: izričite pravne nadležnosti, kada zakon imenuje kontrolora ili daje zadatak ili dužnost prikupiti i obraditi određene podatke, zajedničke zakonske odredbe ili postojeće tradicionalne uloge koje obično podrazumijevaju određenu odgovornost u određene organizacije (npr. poslodavac u odnosu na podatke svojih zaposlenika), činjenične okolnosti i druge elemente (kao što su ugovorni odnosi, stvarna kontrola od strane stranke, vidljivost prema subjektima podataka, itd.).

  Ako nijedna od tih kategorija nije primjenjiva, imenovanje kontrolora treba smatrati "ništavim". Zapravo, tijelo koje nema pravni niti činjenični utjecaj kako bi odredilo kako se obrađuju osobni podaci ne može se smatrati kontrolorom.

  Utvrđivanje "svrhe" obrade pokreće kvalifikaciju za (*zapravo*) kontroler. Umjesto toga, određivanje "sredstava" obrade može delegirati kontrolor, što se tiče tehničkih ili organizacijskih pitanja. Međutim, bitna pitanja koja su bitna za jezgru zakonitosti obrade - kao što su podaci za obradu, duljina skladištenja, pristup itd. - određuje kontrolor.

- *osobni* aspekt definicije odnosi se na široki niz tema koje mogu igrati ulogu kontrolora. Međutim, u strateškoj perspektivi raspodjele odgovornosti, prednost treba dati razmatranju kao kontrolora tvrtke ili tijela kao takvog, a ne određene osobe unutar tvrtke ili tijela. Tvrtka ili tijelo smatraju se odgovornim za obradu podataka i obveze koje proizlaze iz zakonodavstva o zaštiti podataka, osim ako postoje jasni elementi koji ukazuju na to da je fizička osoba odgovorna, na primjer kada fizička osoba koja radi u tvrtki ili javno tijelo koristi podatke za vlastite svrhe, izvan djelatnosti tvrtke.

- Mogućnost *pluralistička kontrola* zadovoljava sve veći broj situacija u kojima različite strane djeluju kao kontrolori. Procjena ove zajedničke kontrole trebala bi odražavati ocjenu "jedinstvene" kontrole, uzimanjem suštinskog i funkcionalnog pristupa i fokusiranjem na to da li svrhe i bitni elementi sredstava određuju više od jedne strane.

Sudjelovanje stranaka u određivanju svrhe i načina obrade u kontekstu zajedničke kontrole može poprimiti različite oblike i ne mora se jednako dijeliti. Ovo mišljenje pruža mnoge primjere različitih vrsta i stupnjeva zajedničke kontrole. Različiti stupnjevi kontrole mogu dovesti do različitih stupnjeva odgovornosti i odgovornosti, a „solidarna“ odgovornost se sigurno ne može pretpostaviti u svim slučajevima. Nadalje, dobro je moguće da u složenim sustavima s višestrukim akterima pristup osobnim podacima i ostvarivanje prava drugih subjekata podataka mogu biti osigurani i na različitim razinama od strane različitih sudionika.

Ovo mišljenje također analizira koncept procesor, čije postojanje ovisi o odluci kontrolora, koja može odlučiti da li će obraditi podatke unutar svoje organizacije ili delegirati sve ili dio aktivnosti obrade vanjskoj organizaciji. Stoga su, s jedne strane, dva temeljna uvjeta za kvalificiranje obrađivača zasebna pravna osoba u odnosu na kontrolora i, s druge strane, obrada osobnih podataka u njegovo ime. Ova aktivnost obrade može biti ograničena na vrlo specifičan zadatak ili kontekst ili može sadržavati određeni stupanj diskrecije o tome kako služiti interesima kontrolora, omogućujući obrađivaču da odabere najprikladnija tehnička i organizacijska sredstva.

Nadalje, uloga obrađivača ne proizlazi iz prirode subjekta koji obrađuje osobne podatke, nego iz njegovih konkretnih aktivnosti u određenom kontekstu te u odnosu na određene skupove podataka ili operacija. Neki kriteriji mogu biti korisni u određivanju kvalifikacije različitih sudionika uključenih u obradu: razine prethodnih uputa koje daje kontrolor podataka; nadzor od strane kontrolora podataka o razini usluge; vidljivost prema subjektima podataka; stručnost stranaka; autonomnost odlučivanja prepuštena različitim stranama.

Rezidualna kategorija "Treća strana"definira se kao bilo koji sudionik koji nema poseban legitimitet ili ovlaštenje - koji bi mogao potjecati, na primjer, od njegove uloge kontrolora, procesora ili njihovih zaposlenika - u obradi osobnih podataka.

* * *

Radna skupina prepoznaje poteškoće u primjeni definicija Direktive u složenom okruženju, gdje se mogu predvidjeti mnogi scenariji koji uključuju kontrolore i procesore, sami ili zajedno, s različitim stupnjevima autonomije i odgovornosti.

U svojoj analizi naglasio je potrebu da se odgovornost raspodijeli na način da će se poštovanje pravila o zaštiti podataka u praksi u dovoljnoj mjeri osigurati. Međutim, on nije našao nikakav razlog da smatra da trenutna razlika između kontrolora i obrađivača više neće biti relevantna i izvodljiva u tom pogledu.

Radna skupina stoga se nada da će objašnjenja dana u ovom mišljenju, ilustrirana konkretnim primjerima iz svakodnevnog iskustva tijela za zaštitu podataka, pridonijeti učinkovitom usmjeravanju na način tumačenja tih temeljnih definicija Direktive.

Sastavljeno u Bruxellesu 16. veljače 2010

Za Radnu skupinu,
predsjedatelj
Jacob KOHNSTAMM