JOGI FÓRUM PUBLIKÁCIÓ

www.jogiforum.hu

A GDPR kínai „unokatestvére”

- avagy a kínai adatvédelmi törvény megszületése és várható hatásai

Szerző:

dr. Kaszián Ábel Gergő

2021. szeptember

A Kínai Népi Kongresszus (National People's Congress - NPC) 2021. augusztus 20-án fogadta el az első átfogó kínai adatvédelmi törvényt, a személyes adatok védelméről szóló törvényt (Personal Information Protection Law - PIPL), kevesebb mint egy évvel azután, hogy a törvény első tervezete megjelent. A novemberben 1-jén hatályba lépő PIPL a harmadik pillére annak a technológiai szabályozási rendszernek, amelyet a Kínai Népköztársaság (a továbbiakban az egyszerűbb megfogalmazás érdekében: Kína) évek óta fejleszt. 2017-ben a kiberbiztonsági törvény (Cybersecurity Law) lefektette a rendszer alapjait, majd 2021 elején elején hatályba lépett az adatbiztonsági törvény (Data Security Law - DSL) új biztonsági keretrendszert határozott meg, amelyet az adatokat kezelő vállalatoknak végre kell hajtaniuk. A jelen írásban a PIPL bemutatása mellett annak az európai általános adatvédelmi rendelethez (General Data Protection Regulation - GDPR) való hasonlóságait és különbségeit elemezzük, továbbá kitekintünk a várható hatásokra is.

1. Előzmények, alapvetés

A PIPL egy kerettörvény, amelynek nem célja, hogy a benne foglalt adatvédelmi szakmai kérdések mindegyikéről részletes leírásokat tartalmazzon, hanem inkább általános elveket, célkitűzéseket és felelősségi köröket határoz meg. Szembetűnő a különbség a GDPR-hoz képest már a terjedelemben is. A PIPL **sem preambulumbekezdéseket, sem fogalommeghatározásokat nem tartalmaz**, így karakterterjedelme a GDPR-énak mintegy tíz százaléka. Ezen általánosságok konkretizálása és pontosítása érdekében a szabályozó hatóságok, például a Kínai Kibertér Hatóság (Cyberspace Administration of China - CAC) **végrehajtási rendeleteket, útmutatókat, a szabványügyi szervezetek pedig technikai szabványokat és előírásokat fognak kiadni**. Mivel tehát a PIPL sokkal rövidebb és kevésbé részletes, mint fő nemzetközi megfelelője, a GDPR, így a szabályozási kérdésekre adott részletes válaszok – nem is beszélve arról, hogy a törvényt hogyan lehet majd végrehajtani – még hónapokig vagy évekig váratnak magukra.

Tagadhatatlan természetesen, hogy a kínai jogalkotók és adatvédelmi szakemberek figyelembe vették a GDPR-t és annak rendelkezéseit, mint az eddigi legnagyobb hatású „privacy"-témájú jogszabályt, azonban az egy az egyben összehasonlítás már csak azért sem állja meg a helyét, mert a gazdasági és társadalmi kontextust is ismernünk kell a jogalkotói célok megértéséhez. Természetesen a GDPR-ral,

mint nemzetközi zsinórmértékkel összehasonlítás kiválóan alkalmas a PIPL jellegzetességeinek megragadására, azt azonban nem szabad feltételeznünk, hogy ez egy „szolgai másolás" eredménye, a Kínai Népköztársaságban (a továbbiakban az észszerű tömörítés érdekében: Kína) igen komoly és felkészült adatvédelmi szakemberek bevonásával készült a jogszabály. **A sajtóban néhol előforduló „kínai GDPR" megnevezés tehát alapvetően félrevezető.**

A PIPL középpontjában az egyének, a társadalom és a nemzetbiztonság védelme áll a személyes adatokkal való visszaéléstől és helytelen adatkezelésből eredő károktól mind a magánszektor, mind a közszféra vonatkozásában azzal, **hogy a kínai törekvés kevésbé az egyének magánélethez való jogának védelmére irányul, mint inkább a nemzetbiztonság és a társadalmi rend megőrzésére**. Ezzel együtt jár, hogy az államnak és az állami szerveknek nagyobb beleszólásuk van az adatok kezelésébe és ezáltal az adatokhoz hozzáférésre is több a lehetőség állami részről, mint ahogyan azt Európában megszokhattuk. Ennek az egyéni szabadságjogokra gyakorolt lehetséges hatásai és kockázatai nem képezik ezen írás tárgyát, de tény, hogy a kínai állampolgároknak egyéni érdekeik védelmében némiképp az európaitól eltérő hozzáállásra és módszerekre lehet szükségük.

2. Célok és tartalmi felépítés

A PIPL **hivatalosan deklarált céljai** a következők:

- az egyének jogainak és érdekeinek védelme;
- a személyes adatok kezelésével kapcsolatos tevékenységek szabályozása;
- az adatok jogszerű és rendezett áramlásának biztosítása;
- a személyes adatok észszerű felhasználásának elősegítése.

A PIPL nyolc érdemi fejezetre oszlik. Az alábbiakban összefoglaljuk a törvény legfontosabb szempontjait, és átfogó elemzést nyújtunk.

I. fejezet: Általános rendelkezések

II. fejezet: Személyes adatok kezelésére vonatkozó szabályok

1. alfejezet: Általános rendelkezések

2. alfejezet: A személyes adatok különleges kategóriájának kezelésére vonatkozó szabályok

3. alfejezet: A személyes adatok állami szervek általi kezelésére vonatkozó különleges rendelkezések

III. fejezet: A személyes adatok határokon átnyúló szolgáltatására vonatkozó szabályok

IV. fejezet: Az egyének jogai a személyes információk kezelésével kapcsolatos tevékenységek során

V. fejezet: A személyes információk kezelőinek (ti. az adatkezelőknek) kötelezettségei

VI. fejezet: A személyes adatok védelmével kapcsolatos feladatokat és kötelezettségeket ellátó szervezeti egységek

VII. fejezet: Jogi felelősség

VIII. fejezet: Kiegészítő rendelkezések

Kedvcsinálóként pár kiemelt érdeklődésre számot tartó téma:

- **a személyes adatok meghatározása tág**, mint a GDPR-ban, azaz minden idetartozik, ami azonosít egy személyt;
- **extraterritoriális hatállyal is bír**, amely jelentős, hiszen a GDPR is ennek „köszönhette", hogy világszerte megkerülhetetlenné vált, emellett a határokon átnyúló adattovábbítás mechanizmusairól is rendelkezik;
- meghatározott esetekben **adatvédelmi tisztviselőt kell kinevezni**;
- a GDPR-ban megtalálhatóhoz nagyban hasonló **adatkezelési jogalapokat határoz meg;**
- **egyéni jogokat biztosít az érintetteknek** (az „érintett" és az „egyén" kifejezéseket a könnyeb érthetőség kedvéért a jelen írásban szinonimaként használjuk, értve ez alatt azon természetes személyeket, akik személyes adatai az adatkezelésekkel érintettek; a szövegben „individuals", a GDPR szóhasználatában „data subjects"), beleértve azt a jogot, hogy az adatkezelőtől az adatkezelési szabályok magyarázatát kérjék;
- **szabályozza az arcfelismerő technológia közterületi használatát;**
- megköveteli az adatkezelőktől a kiberbiztonsági intézkedéseket és a rendszeres felülvizsgálatot;
- 50.000.000 kínai jüanig (kb. 7.700.000 USA dollár) vagy a vállalat tavalyi forgalmának 5%-áig terjedő **adatvédelmi bírság kiszabására ad lehetőséget**;
- **személyes felelősséget ró a vállalati döntéshozókra**, vezető tisztségviselőkre és adatvédelmi tisztviselőkre, a szankció lehet pénzbírság vagy a munkaviszony felfüggesztése is.

A főbb fejezeteket áttekintve a következő megállapításokat tehetjük, az alábbi témák mentén.

3. Alapfogalmak

Rögtön az elején szembetűnő, ahogy a bevezetőben már említettük, hogy sem az értelmezést segítő preambulumbekezdéseket, sem fogalommagyarázatokat nem találunk. Utóbbi a GDPR 4. cikkében megjelenik és általánosan bevett az európai jogalkotásban. A PIPL-ben ezzel szemben a fogalmakat a szövegben elszórtan találhatjuk meg azzal, hogy azok sok esetben a GDPR-ral jelentős hasonlóságot mutatnak, azonban az egyes megfogalmazásbeli, apró eltérések mögötti szándék nem minden esetben egyértelmű.

3.1. A személyes adatok általános meghatározása

Kezdjük a személyes adat meghatározásával. A PIPL 4. cikke szerint **az bármely elektronikus vagy más módon rögzített információ, amely egy azonosított vagy azonosítható természetes személyre vonatkozik**. Ez a meghatározás nagymértékben tükrözi a kiberbiztonsági törvényben és a kínai polgári törvénykönyvben foglalt meghatározást, amelyek a személyes adat fogalmát különböző típusú elektronikus vagy más módon rögzített információkként határozzák meg, amelyek külön-külön vagy más információkkal kombinálva felhasználhatók a természetes személy azonosítására. Nagy a hasonlóság a GDPR meghatározásával, amely szerint személyes adat az „azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ”.

3.2. A személyes adatok különleges kategóriái

A törvény továbbá meghatározza, hogy a személyes adatok különleges kategóriái (a PIPL szóhasználatával „érzékeny adatok”, a jelen írásban ezért ezeket szinonimaként használjuk) olyan adatokat jelentenek, amelyek nyilvánosságra kerülése vagy jogellenes felhasználása az egyénekkel szembeni megkülönböztetést vagy a személyi vagy vagyonbiztonság súlyos sérelmét okozhatja, beleértve **a faji, etnikai, vallási meggyőződésre, egyéni biometrikus jellemzőkre, egészségi állapotra, pénzügyi számlákra, egyéni helymeghatározásra stb. vonatkozó információkat**. (Szerzői megjegyzés: a „stb.” alkalmazása nem pontatlanság, hanem a PIPL fordításának idézése, amely ezen

esetben nyitott végű felsorolást jelent.) Az adatkezelők ezeket az érzékeny személyes adatokat csak meghatározott célból és csak akkor kezelhetik, ha az megalapozottan szükséges. Az adatkezelőknek továbbá külön – akár írásos – hozzájárulást kell beszerezniük, ha az adatkezeléshez egyéni hozzájárulásra támaszkodnak (PIPL 28-30.).

A személyes adatok különleges kategóriájának kezelése eltér a GDPR 9. cikkének szemléletétől, ahol egy zárt lista található, vagyis kizárólag ezekben az esetekben kezelhetőek ilyen adatok, egyebekben azok kezelése tilos. **A PIPL viszont az érzékeny adatok nyílt listáját tartalmazza**, és a meghatározás középpontjában az egyéni sérelem fogalma és az adatok egyénekre gyakorolt potenciális diszkriminatív hatása áll. A GDPR 10. cikkében foglaltakkal ellentétben a PIPL nem tartalmaz külön rendelkezést a bűncselekményekre vonatkozó személyes adatok kezelésére vonatkozóan, viszont a pénzügyi információkat és a helymeghatározási adatokat az érzékeny személyes adatok körébe sorolja.

3.3. Az azonosítástól való megfosztás és az anonimizálás meghatározása

A „azonosítástól való megfosztás" („de-identifikáció"), továbbá az az „anonimizálás" fogalmát a PIPL legutolsó érdemi rendelkezése határozza meg (PIPL 73.), az anonimizált személyes adatok pedig kifejezetten ki vannak zárva a törvény tárgyi hatálya alól (PIPL 4.), a GDPR 26. preambulumbekezdéséhez hasonlatosan. A „de-identifikáció" a GDPR „álnevesítés" fogalmával állítható párhuzamba.

A PIPL a de-identifikációt nem magyarázza bővebben, hanem csak azon technikai biztonsági intézkedések közé sorolja, amelyeket a személyes adatok kezelői a biztonsági kötelezettségeknek való megfelelés érdekében alkalmazhatnak (PIPL 51.).

3.4. Az adatkezelés fogalmának kiterjesztő értelmezése

A PIPL adatkezelés-fogalma magában foglalja a személyes adatok „gyűjtését, tárolását, felhasználását, feldolgozását, továbbítását, rendelkezésre bocsátását, közzétételét és egyéb hasonló tevékenységeket" (PIPL 4.). Ez hasonlít a GDPR szerinti meghatározásához, amely szerint a

törvényben meghatározott szabályok a személyes adatok gyűjtésére és felhasználására egyaránt vonatkoznak, vagyis az adatok útját végigkísérik a „születéstől” kezdve. A törvény tartalmazza az adatkezelési jogalapokat is, amelyeknek már az adatkezelés megkezdése előtt megalapozottan rendelkezésre kell állniuk.

4. Az adatkezeléssel érintett felek

4.1. Adatkezelők és adatfeldolgozók

Elöljáróban megjegyzendő, hogy sem a PIPL, sem más kínai jogszabály nem használja kifejezetten az „adatkezelő” kifejezést, a „controller” helyett a „personal information handler” használatos. Az adatkezelésre a „processing” kifejezést alkalmazza, amely európai szemmel elsőre oda nem illőnek tűnhet, mivel a „processor” a GDPR szóhasználatában az „adatfeldolgozó”-ra értendő. Ez utóbbit a PIPL angol fordítással „trustee / entrusted person”-ként jeleníti meg, legelőször a PIPL 21-ben.

A PIPL szerint **a felek vagy személyek akkor válnak adatkezelővé, ha „önállóan határozzák meg a személyes adatok kezelésének céljait és eszközeit”** (PIPL 73.). Ez gyakorlatilag azonos a GDPR 4. cikke 7. pontjának fogalmával („az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait”).

Az adatkezelők tehát a személyes adatok kezelését harmadik félre bízhatják **a GDPR-ban szereplő adatkezelő-adatfeldolgozó kapcsolathoz nagyon hasonló feltételek mellett**. Megállapodást kell kötniük, amelynek ki kell térnie az adatkezelés céljára, a kezelési módszerre, a személyes adatok kategóriáira, mindkét fél jogaira és kötelezettségeire, beleértve az adatfeldolgozó tevékenységének felügyeletét is (PIPL 22.). Végül, ha a harmadik féllel kötött adatkezelési megállapodás érvénytelenné válik, vagy más módon megszűnik, a harmadik fél nem tárolhatja a személyes adatokat, és vagy visszaadja azokat az adatkezelőnek, vagy törli azokat (PIPL 21.).

A törvény a közös adatkezelésre vonatkozó szabályokat is meghatározza, a közös adatkezelőknek meg kell állapodniuk az egyes kezelők jogairól és kötelezettségeiről, és a megállapodás pedig nem

érintheti az egyén azon lehetőségét, hogy bármelyikükkel szemben gyakorolja jogait; a jogsértésekért szintén közösen felelnek (PIPL 21.). Ez gyakorlatilag egyezik a GDPR 26 cikkében foglaltakkal.

4.2. Mentesség, a köz- és magánszféra szereplőire vonatkozó szabályok

A GDPR 2. cikkében foglalt személyes vagy otthoni adatkezelési tevékenységekre vonatkozó mentességéhez hasonlóan **a PIPL sem vonatkozik a természetes személyek által személyes vagy családi ügyeikben végzett adatkezelésre** (PIPL 72.). A PIPL továbbá a magán- és a közszférában végzett adatkezelési tevékenységekre egyaránt vonatkozik. Egyrészt egyetlen magánszervezet sem mentesül a törvény hatálya alól; másrészt bizonyos vállalatokra (azok, amelyek kiemelt fontosságú, internetes platformszolgáltatásokat nyújtanak, nagyszámú felhasználót és összetett adatkezelést végeznek) fokozott kötelezettségek vonatkoznak. Azt, hogy ez pontosan milyen személyi kört érint, még nem ismerjük.

A közszférában az állami szerveknek (azaz központi, tartományi vagy önkormányzati szintű hatóságoknak és ügynökségeknek, beleértve a bíróságokat és a jogalkotó szerveket is) meghatározott követelményeknek kell eleget tenniük a személyes adatok kezelése tekintetében a jogszabályban előírt feladataik ellátása során (PIPL 34.). Ezek a szabályok a kínai közigazgatásra vonatkozó, már hatályos adatkezelési szabályokkal együtt alkalmazandók. Ugyanezek a kötelezettségek vonatkoznak azokra a szervezetekre is, amelyek az állami szervek nevében, külön törvények vagy rendeletek alapján kezelik a személyes adatokat (PIPL 37.). Ez utóbbi rendelkezés tipikus a PIPL-ben, amikor egyéb végrehajtó jogszabályokra utalja a részletszabályok kidolgozását.

A kötelezettségek magukban foglalják az érintettek értesítését és hozzájárulásuk beszerzésének szükségességét a személyes adatok kezeléséhez (így például a személyes adatok állami szervek közötti megosztásához), kivéve, ha az értesítés akadályozná a jogszabályi kötelezettségek teljesítését, vagy titoktartási kötelezettség áll fenn (PIPL 18. és 35.). **Az állami szerveknek az általuk kezelt személyes adatokat Kínában („mainland China") kell tárolniuk. A külföldre irányuló adattovábbítás csak azt követően lehetséges, ha megállapításra került, hogy ez valóban szükséges és indokolt, továbbá, miután biztonsági kockázatértékelésen esett át az adatkezelő, az állami felügyeleti szervek közreműködésével (PIPL 36.).** Ezen rendelkezéssel a kínai állam erős kontroll

alatt tudja tartani az adatok kiáramlását, így nagyfokú és nagy sűrűségű adatlokalizációt megvalósítva, amelyben a GDPR vagy akár az európai nemzeti szabályok is sokkal megengedőbbek.

Azok az állami szervek, amelyek nem követik a szabályokat, hatósági vizsgálatot kockázatnak és módosítaniuk kell az adatkezelési folyamataikon. Továbbá, a nemmegfelelőségért felelős személyek egyéni felelősséggel is tartoznak és szankciókra számíthatnak (például jogviszony megszüntetése, pénzbírság). (PIPL 67-68.)

5. Területi hatály, extraterritorialitás

A PIPL tehát alapvetően minden olyan szervezetre vagy személyre vonatkozik, amely fizikailag a Kínai határain belül létezik vagy tartózkodik. **A PIPL 3. ugyanakkor a GDPR-hoz hasonlóan kiterjeszti a törvény területi hatályát a Kínaion kívül letelepedett adatkezelők által végzett adatkezelési tevékenységekre,** amennyiben az alábbi körülmények valamelyike fennáll:

- ha a cél a Kína határán belüli természetes személyek számára történő termék- vagy szolgáltatásnyújtás;
- amennyiben a határokon belül lévő természetes személyek tevékenységeinek elemzése vagy értékelése történik;
- törvényekben vagy közigazgatási rendelkezésekben meghatározott egyéb körülmények.

Ennek a harmadik bekezdésnek sincsen közvetlen megfelelője a GDPR-ban, és mérlegelési mozgásteret hagy a hatóságoknak arra, hogy a törvény extraterritoriális karját „tovább nyújtsák”.

A törvény ezen felül előírja, hogy a Kínán kívüli adatkezelőknek az országon belül külön szervezetet kell létrehozniuk vagy képviselőt kell kinevezniük, aki az adatkezeléssel kapcsolatos ügyekért felelős (PIPL 52.), továbbá meg kell adniuk a képviselő nevét és elérhetőségét a törvény végrehajtásáért felelős illetékes hatóságoknak.

6. Jogalapok

Adatkezelésre az alábbi jogalapok állnak rendelkezésre (PIPL 13.):

- az egyének **hozzájárulásának** beszerzése;
- amennyiben olyan **szerződés megkötéséhez vagy teljesítéséhez szükséges** az adatkezelés, amelyben az egyén érdekelt fél, vagy amennyiben a vonatkozó munkaügyi szabályoknak való megfeleléshez, kollektív szerződés végrehajtásához vagy humán erőforrás kezeléséhez (pl. munkavállalók adatai) szükséges;
- amennyiben **jogszabályi kötelezettségek teljesítéséhez** szükséges;
- amennyiben **váratlan közegészségügyi események okán vagy a természetes személyek életének és egészségének, illetve vagyonának megóvása érdekében** szükséges;
- a személyes adatok észszerű keretek között történő kezelése a **híradás-tudósítás, közvélemény-kutatás vagy más közérdekű cél** érdekében;
- az egyén által vagy más módon **jogszerűen nyilvánosságra hozott** adatok észszerű keretek között történő kezelése, kivéve, ha az egyén kifejezetten tiltakozik, vagy, ha ez jelentős hatással van az egyén érdekeire;
- **törvényekben és közigazgatási határozatokban meghatározott** egyéb körülmények.

Ahogy a GDPR-ban, úgy **itt sincsen preferált sorrend a jogalapok között**. Ennek jelentősége, hogy a korábbi kínai szabályozásban (beleértve a kiberbiztonsági törvényt és a polgári törvénykönyvet) mindig a hozzájárulás volt az elsődleges jogalap. A piaci szereplők számára ez kedvező változás és többéves lobbi eredménye, sokan érveltek már a szerződés teljesítésén és a jogos érdeken alapuló jogalapok bevezetése mellett.

A siker ugyanakkor nem teljes, **a jogalap-lista ugyanis nem tartalmazza a jogos érdek fogalmát,** amely már évtizedek óta része az európai adatvédelmi rendszernek, és több Európán kívüli jogrendben is jelen van, többek között Ázsiában is. Az ehhez legközelebb álló rendelkezés a fent idézett PIPL 13. (2) bekezdése, ahova bekerült a munkavállalók adatainak kezelése, mint a hozzájárulástól elkülönülő és meghatározott érdeken alapuló jogalap.

6.1. Hozzájárulás-központúság

A jogalapok körének szélesítésével párhuzamosan mindazonáltal továbbra is általánosan jellemző a jogszabályra **a hozzájárulás-központúság**. A PIPL 25. alapján tiltott például, hogy az adatkezelők nyilvánosságra hozzák az általuk kezelt személyes adatokat, kivéve, ha ehhez külön hozzájárulást kapnak. A nyilvánosan hozzáférhető személyes adatok feldolgozása során pedig csak olyan adatkezelés végezhető, amely megfelel annak a célnak, amely alapján az adatokat eredetileg közzétették, és ha az adatkezelési cél ettől eltér, az érintetteket értesíteni kell és hozzájárulásukat kell kérni. A közterületen folytatott arcfelismerés esetében is megjelenik a hozzájárulás, akként, hogy ezen tevékenység folytatása csak a közbiztonság biztosítása céljából megengedett, kivéve ha az érintettek külön hozzájárulnak az ettől eltérő célú adatkezeléshez (PIPL 26.).

A **hozzájárulás érvényességének feltételei** a következők: a hozzájárulásnak tájékozottnak kell lennie, az adatkezelésről való előzetes tudomásszerzés mellett – a GDPR 13. cikkével egybehangzóan –, és azt önkéntes, kifejezett akaratnyilatkozatban kell megadni. További jogszabályok megkövetelhetik a külön írásbeli hozzájárulást (PIPL 14.).

A GDPR 7. cikkében foglaltakhoz hasonlóan az érintetteknek joguk van a hozzájárulás visszavonására (PIPL 15.). A GDPR 7. cikke (4) bekezdésében foglaltakhoz hasonlóan a PIPL is előírja, hogy az adatkezelők nem tagadhatják meg a termékek vagy szolgáltatások nyújtását azon az alapon, hogy az érintett nem járul hozzá az adatkezeléshez, vagy visszavonja hozzájárulását, kivéve azokat a helyzeteket, amikor a személyes adatok szükségesek a termékek vagy szolgáltatások nyújtásához (PIPL 16.). Az adatkezelőknek kellően egyszerű és elérhető („convenient”) módot kell biztosítaniuk az egyének számára a hozzájárulás visszavonására, és a visszavonás nem érinti a hozzájárulás visszavonása előtt végzett adatkezelést (15. cikk).

6.2. Gyermekekre vonatkozó szabályok

A 14 évnél fiatalabb gyermekek személyes adatait kezelőknek be kell szerezniük a szülők hozzájárulását (PIPL 31.). A GDPR 8. cikke előírja a 16. életévét be nem töltött gyermek esetén, hogy a gyermekek személyes adatainak kezelése csak akkor és olyan mértékben jogszerű, ha a hozzájárulást a gyermek feletti szülői felügyeletet gyakorló adta meg, illetve engedélyezte, azzal,

hogy a tagállamok e célokból jogszabályban ennél alacsonyabb, de a 13. életévnél nem alacsonyabb életkort is megállapíthatnak. Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) nem tartalmaz külön a gyermekekre vonatkozó rendelkezéseket.

6.3. Alapelvek

- Az „őszinteség" és „jóhiszeműség" elve - amely a GDPR tisztességes eljárás elvével rokon. A törvény ismeri továbbá a jogszerűség és a szükségesség elvét is (PIPL 5.);
- célhoz kötöttség, beleértve azt a követelményt, hogy a személyes adatkezelés egyértelmű, észszerű és közvetlenül releváns céllal történje; létezik továbbá adatminimalizálási rendelkezés is (PIPL 6.);
- nyitottság és az átláthatóság (PIPL 7.);
- pontosság és az elszámoltathatóság (PIPL 8-9.), amely utóbbi a GDPR-nak is jelentős újítása volt;
- korlátozott tárolhatóság (PIPL 19.); a megőrzési idő az adatkezelési cél megvalósításához szükséges lehető legrövidebb időtartam.

7. Automatizált döntéshozatal és arcfelismerés

A PIPL szerint az automatizált döntéshozatal (automated decision-making - ADM) alatt olyan tevékenységeket kell érteni, **amelyek személyes adatokat használnak fel az egyéni viselkedés és szokások, érdeklődési körök, hobbik, illetve pénzügyi, egészségügyi vagy hitelképességi helyzetek automatikus elemzésére, értékelésére és számítógépes programok segítségével történő eldöntésére. [PIPL 73. (2)].**

A jogszabály konkrét kötelezettségeket is előír:

- ADM esetén az adatkezelőknek garantálniuk kell az átláthatóságot, a tisztességességet és az eredmény észszerűségét (PIPL 24.). Ha az érintett úgy véli, hogy az ADM jelentős befolyást gyakorol a jogaira és érdekeire, magyarázatot kérhet, és elutasíthatja az ADM kizárólagos alkalmazását. Ez egybevág a GDPR 21. cikkében foglalt érintetti joggal;

- az ADM-et célzott marketingajánlatok készítéséhez használó szervezeteknek egyúttal lehetőséget kell biztosítaniuk az érintettek számára, hogy ne személyes jellemzők alapján kapjanak ajánlatokat, vagy egyszerű és elérhető tiltakozási módot kell biztosítaniuk (PIPL 24.);
- az ADM révén nem lehet indokolatlanul eltérő tranzakciós árat vagy bánásmódot alkalmazni az érintettekkel szemben (PIPL 24.);
- az adatkezelőknek adatvédelmi hatásvizsgálatot kell végezniük, mielőtt ADM-alapon szolgáltatásokat kínálnak (PIPL 55.), a GDPR 35. cikkével összhangban.

7.1. Arcfelismerési szabályok a nyilvános helyeken

Közterületen a képgyűjtő vagy személyazonosság-felismerő berendezéseket csak a közbiztonság védelme és a vonatkozó jogszabályok betartása érdekében lehet alkalmazni (PIPL 26.). **A közbiztonság védelme az egyetlen elismert jogalap, továbbá követelmény, hogy az érintetteket értesíteni is kell az információgyűjtési folyamatról**, a jogszabály szerint praktikusan jelzésekkel vagy táblákkal („signs"). Az ilyen módon gyűjtött információkat nem lehet közzétenni vagy nyilvánosságra hozni, kivéve, ha az egyének külön beleegyezésüket adták, vagy ha a jogszabályok másként rendelkeznek. Ahogyan erre már korábban utaltunk, a hozzájárulás-központú szemlélet itt is visszaköszön.

A rendelkezések mutatják **a kínai közvéleményben is egyre erősődő tudatosságot azzal összefüggésben, hogy az arcfelismerő technológiák nyilvános használata az érintettek számára is jelentős érdeksérelemmel járhat,** így minél pontosabb szabályozásra van szükség. Egy híres, a Kínán belül és kívül is nagy visszhangot kiváltó ügyben például egy egyetemi oktató, Guo Bing keresetet indított a Hangzhou Safari Parkkal szemben, mert az az arcfelismerő technológiát a vendégek megfigyelésére és beengedésére használta. A Parknak végül a bíróság döntése értelmében törölnie kellett a felperes arcnyomatát. Ezen kívül több város is elfogadott olyan rendeleteket, amelyek korlátozzák vagy tiltják e technológiák használatát, köztük Tianjin, Nanjing és Xuzhou.

8. Az egyének jogai (hozzáférés, törlés, hordozhatóság, a magyarázathoz való jog)

A PIPL értelmében **az egyéneknek az adatkezelés megkezdése előtt kifejezett tájékoztatást kell kapniuk**, amely tartalmazza az adatkezelő személyazonosságát és elérhetőségét, az esetleges harmadik feleket, adatfeldolgozókat, az adatkezelés célját és módszereit, a kezelt személyes adatok kategóriáit, a megőrzési időt, valamint az egyéni jogérvényesítés lehetőségeit (PIPL 17.). Ez a GDPR 13. cikkével állítható párhuzamba.

A PIPL 18. cikke kimondja, hogy az adatkezelőknek nem kell értesíteniük az érintettet, ha államtitok sérülne ezáltal, vagy veszélyhelyzeti körülmények között, amelyek közé tartozhat a közbiztonság vagy a közegészség veszélyeztetése.

A PIPL előírja, hogy az adatkezelőknek **eljárásokat kell létrehozniuk az érintetti joggyakorlás elősegítésére** (PIPL 50.) és az erre irányuló irányuló kérelmeket csak indokkal utasíthatják el, ez esetben pedig az érintettek belátásuk szerint bírósághoz fordulhatnak.

A PIPL a következő **érintetti jogokat** ismeri:

- A mások általi adatkezelés megismeréséhez, az arról való döntéshez, a visszautasításhoz és az adatkezelés korlátozásához való jog (PIPL 44.);
- a hozzáféréshez és másolathoz való jog (PIPL 45.);
- a kijavításához vagy kiegészítéséhez való jog (PIPL 46.);
- a törléshez való jog, ha
    - a megőrzési idő eltelt vagy az adatkezelés célja megvalósult;
    - az adatkezelő a szolgáltatást megszünteti;
    - az érintett visszavonja hozzájárulását;
- az adatkezelés jogszabálysértő (PIPL 47.);
- kijelölt adatkezelőhöz történő adattovábbítás joga [PIPL 45. (3) bekezdés]. Az adatok áthelyezésének konkrét feltételeit az állami kiberbiztonsági és információs szervek határozzák meg a későbbiekben;
- az adatkezelési eljárások magyarázatához való jog (PIPL 48.).

Ezek **a jogok az érintett halála után is gyakorolhatók közeli hozzátartozói által**, kivéve, ha még életében másként rendelkezik (PIPL 49.). Megjegyezzük, hogy a GDPR ezzel szemben az elhunyt személyek adatkezelésével kapcsolatos szabályozást tagállami hatáskörbe helyezi. Lásd még a GDPR 27. preambulumbekezdését és ezzel összefüggésben az információs önrendelkezési jogról és az Infotv. 25. §-át.

9. Elszámoltathatóság: adatvédelmi hatásvizsgálat, adatvédelmi tisztviselő, incidens-bejelentés, képzési kötelezettségek, nagymértékű adatkezelési műveletek.

A PIPL 52. előírja, hogy **az illetékes hatóságok által meghatározott mértéket (mennyiséget) elérő adatkezelőknek ki kell jelölniük a személyes adatok védelméért felelős személyeket**, és közzé kell tenniük e személyek nevét és elérhetőségét. Ha az adatkezelő incidenst észlel, haladéktalanul helyreállító intézkedéseket kell hoznia, és értesítenie kell az illetékes hatóságokat (PIPL 57.). Amennyiben az elfogadott intézkedésekkel hatékonyan el lehet kerülni az incidensek okozta károkat, az adatkezelőknek nem kell értesíteniük az érintetteket. Ez a rendelkezés is nagyban hasonlít a GDPR 34. cikkének szabályozására.

Az adatkezelőknek **adatvédelmi hatásvizsgálatot kell végezniük** annak megállapítására, hogy az adatkezelés céljai és módszerei jogszerűek-e, az adatkezelés milyen hatással van az érintettekre, továbbá, hogy az elfogadott biztonsági intézkedések megfelelőek-e (PIPL 55.). A hatásvizsgálatnak figyelembe kell vennie az érzékeny személyes adatok kezelését, az automatizált döntéshozatalt, az adatfeldolgozást, a határokon átnyúló adattovábbítást és más, érintetti jogokra és érdekekre jelentős hatást gyakorló adatkezelési tevékenységeket. Az adatkezelőknek továbbá **megfelelő technikai-biztonsági intézkedéseket kell alkalmazniuk**, így titkosítást, anonimizálást; meg kell határozniuk az adatkezelés korlátait, és rendszeresen biztonsági képzést kell tartaniuk a munkavállalók számára. Ezen túlmenően meg kell fogalmazniuk és meg kell szervezniük az incidens-reagálási tervek végrehajtását. Kötelezettség még, hogy **rendszeresen auditáltatni kell az adatkezelési tevékenységeiket az illetékes hatóságokkal** (PIPL 54.). Ez utóbbi rendelkezés várhatóan komoly terhet ró majd a hatóságokra, azzal együtt is, hogy a gyakoriság mértéke jelenleg még nem ismert. Európából tekintve, minden egyes adatkezelőre vonatkoztatva ezen előírást, igen komoly adminisztráció -és erőforrás-igényes rendelkezésnek látszik.

A törvény egyik új rendelkezése – amely az utolsó pillanatban került be a szövegtervezetbe – a nagy online platformokat célozza meg konkrét kötelezettségekkel. Megjegyezzük, hogy ezen online platformokra vonatkozó külön szabályozás az Európai Unióban sem ismeretlen, jelenleg az Európai Bizottság által a 2020. december 15-én bemutatott, a digitális szolgáltatások egységes piacáról szóló jogszabálycsomagjára (Digital Services Act - DSA) tartalmaz erre vonatkozó rendelkezéseket.

A PIPL ezen új rendelkezései **előírják a nagyszámú felhasználónak platformszolgáltatást nyújtó és összetett üzleti típusokkal rendelkező adatkezelők számára**, hogy

- független szervezetet hozzanak létre az adatkezelési tevékenységek felügyeletére;
- kövessék a nyitottság, a méltányosság és az igazságosság elveit;
- súlyos jogsértés esetén haladéktalanul hagyjanak fel a szolgáltatásnyújtással; és
- rendszeresen tegyenek közzé jelentéseket az adatkezelők társadalmi felelősségvállalásáról (PIPL 58).

Az utóbbi pont értékes etikai többlettartalommal bír, a CSR (Corporate Social Responsibility) törvényi szintre emelésével az adatvédelemben, érdekes lesz látni, hogyan alakítják ezen jelentésüket az adatkezelők, illetve, hogy lesznek-e konkrét tartalmi vagy formai elvárások az illetékes hatóságok részéről.

10. Határokon átnyúló adattovábbítás és adatlokalizálás

Ez a fejezet jól példázza a szöveg által követett célok sokféleségét, mivel a jogalkotó egyszerre törekszik a kínai polgárok jogait és érdekeit tiszteletben tartó, felelősségteljes adattovábbítás előmozdítására és a kínai stratégiai érdekek védelmére.

Az adatok Kína határain kívülre történő továbbítását a III. fejezet szabályozza, azzal az alapelvvel, hogy **az adatokat a Kínán kívülre továbbítást követően is ugyanolyan védelemben kell részesíteni**. A GDPR 44. cikke, illetve az Európai Unió Bírósága által a Schrems-ügyekben többször értelmezett, „lényegében azonos", elvárt védelmi szint tehát itt is visszaköszön.

Minden adattovábbításnak **meg kell felelnie a szükségességi tesztnek** – az „üzleti szükségesség" jelentése jelenleg nincs kitöltve tartalommal. Ezenkívül az adatkezelőknek – az adattovábbítást megelőzően – külön értesítést kell küldeniük az érintetteknek, függetlenül attól, hogy milyen adattovábbítási mechanizmust alkalmaznak, és az értesítést követően be kell szerezniük az érintett külön hozzájárulását is. A tájékoztatásnak többek között ki kell térnie arra, **ki az adatok címzettje és milyen adatkezelési műveleteket hajt majd végre** (PIPL 39.).

Az adattovábbításnak meg kell felelnie az alábbi feltételek legalább egyikének (PIPL 38.):

- A kiberbiztonsági és informatikai **felügyeleti hatóságok által a PIPL 40. alapján szervezett biztonsági értékelésen sikeresen átesett** az adatkezelő. A rendelkezés rögzíti még, hogy a kritikus információs infrastruktúrák üzemeltetőinek és a nagy mennyiségű személyes adatot továbbító szervezeteknek helyben (értsd: országhatáron belül) kell tárolniuk a Kínában gyűjtött személyes adatokat, és szükség esetén további biztonsági értékelésen kell átesniük az átadáshoz;
- a felügyeleti hatóságok által meghatározott követelmények szerinti, **szakosított szerv által kibocsátott tanúsítvány megszerzése**. A PIP 38. (2) bekezdése tükrözi a GDPR 46. cikk (2) bekezdés f) pontja szerinti „jóváhagyott tanúsítási mechanizmusokra" vonatkozó rendelkezését;
- **szerződés megkötése a külföldi fogadó féllel, amely meghatározza mindkét fél jogait és kötelezettségeit,** és felügyeli tevékenységüket annak biztosítása érdekében, hogy azok megfeleljenek a jogszabályi előírásoknak. A felügyeleti hatóságok általános szerződési feltételeket – ezek megfelelői az EU-ban a transzatlanti adattovábbításokból már jól ismert Standard Contractual Clause-ok (SCC-k) – bocsátanak az adatkezelők rendelkezésére, amelyekre azok határokon átnyúló átadási megállapodások megkötésekor hivatkozhatnak (PIPL 38.);
- a törvényekben vagy közigazgatási rendeletekben vagy a felügyeleti hatóságok által előírt egyéb feltételeknek való megfelelés.

E rendelkezések mindegyike teret nyit a nemzetközi tárgyalások számára a Kína területén, kínai állampolgároktól gyűjtött személyes adatok országon kívüli továbbításáról. Ahogy a PIPL 12. fogalmaz:

„az állam elő kívánja segíteni a személyes adatok védelmére vonatkozó szabályok kölcsönös elismerését, más országokkal és nemzetközi szervezetekkel együttműködésben”.

Érdekes módon ugyanakkor a határokon átnyúló adattovábbításról szóló fejezetben **nem szerepel a GDPR 45. cikkéből ismert „megfelelőségi határozat” alapján történő adattovábbítás lehetősége**. Ezt a választást a PIPL kidolgozói kétségtelenül alaposan megfontolták, és befolyásos kínai akadémikusok munkájára vezethető vissza, akik mind az Európai Unió, mind az Amerikai Egyesült Államok megfelelőségi határozatokon alapuló adattovábbítási modelljére úgy tekintenek, amely szükségtelenül korlátozza és „megmerevíti” az adattovábbításokat, meghatározott földrajzi irányokat és partnereket tartósan előnyben részesítve. Kína ezzel szemben várhatóan a saját érdekeinek rugalmasabb érvényesítésével kíván operálni.

Ha nemzetközi igazságügyi segítségnyújtás vagy bűnüldözés céljából szükséges a személyes adatok Kínán kívülre történő továbbítása, az adatkezelőknek kérelmet kell benyújtaniuk az illetékes hatósághoz jóváhagyás céljából (PIPL 41.). A törvény kimondja, hogy a nemzetközi szerződések vagy megállapodások, amelyeknek Kína részes fele lett, szabályozhatják a határokon átnyúló adattovábbítást, és a törvény rendelkezéseinek helyébe léphetnek. Nem világos ugyanakkor, hogy ez a rendelkezés csak a nemzetközi jogsegélyre vonatkozik-e, vagy a határokon átnyúló adattovábbításokra általánosságban kiterjed. A PIPL előírja, hogy **amennyiben egy ország vagy régió az adatvédelem területén Kínával szemben diszkriminatív tilalmakat, korlátozásokat vagy más hasonló intézkedéseket fogad el, Kína ellen- intézkedéseket hozhat az említett országgal vagy régióval szemben** (PIPL 43.).

Egyértelmű tehát, hogy minden, Kínával és a kínai állampolgárokkal kapcsolatba kerülő adatkezelőnek különös figyelmet kell tanúsítania a törvény betartása érdekében, mivel a kínai polgárok jogait és érdekeit sértő vagy Kína nemzetbiztonságát vagy közérdekét veszélyeztető módon **adatkezelést végző külföldi szervezetek vagy személyek felkerülhetnek egy nyilvánosan elérhető „feketelistára”, amelynek eredményeként adatfogadó félként nem léphetnek fel**, ezzel értelemszerűen komoly üzleti érdeksérelmet szenvedve (PIPL 42.).

11. Végrehajtás, szankciók

A törvény **nem hoz létre kifejezetten az adatvédelmi szabályozás érvényesítésével foglalkozó új hatóságot**. A végrehajtásáért felelős szerv elsősorban a már említett **Kínai Kibertér Hatóság.**

A PIPL szankciókat ír elő a jogsértések és a meg nem felelés esetére, így például **jogellenes adatkezelések felfüggesztésére vagy megszüntetésére** is van lehetőség. A meg nem felelés alatt nemcsak a személyes adatok jogellenes kezelése értendő, hanem az is, ha az adatkezelő nem biztosítja a jogszabályokban előírt védelmi intézkedések folyamatos fennállását.

A törvény kétféle jogsértést különböztet meg. Az első esetben a felügyeleti hatóságok **az adatkezelési műveletek módosítását rendelhetik el, valamint elkobozhatják a jogellenes adatkezelési tevékenység folytatásából származó bevételeket, és figyelmeztetésben részesíthetik az adatkezelőt**. A második esetben a nemzetbiztonságot vagy a közérdeket sértő adatkezelés is jogsértésnek minősül (PIPL 10.), azzal, hogy erre a PIPL nem rögzít vagyoni szankciót. Ekkor **a törvény megsértését nyilvánosan rögzítik, továbbá a felelős személy munkaviszonyának felfüggesztéséhez vezethet**.

A **bírságösszegek** a következőképp alakulnak:

- Ha az adatkezelő megtagadja a jogsértő magatartás abbahagyását, akkor legfeljebb 1.000.000 kínai jüan (kb. 150.000 dollár) összegű bírságot szabnak ki rá;
- a közvetlenül felelős személyek és döntéshozók 10.000 és 100.000 kínai jüan (kb. 1.500-15.000 USA dollár) közötti bírságot is kaphatnak;
- súlyos jogsértések esetén a bírság 50.000.000 RMB-ig (7.500.000 USA dollár) vagy az előző pénzügyi éves bevételének 5%-áig növelhető (PIPL 66.). Zárójeles megjegyzés: a törvény nem határozza meg, hogy az éves bevételt a globális forgalom alapján számítják-e ki.

A PIPL alapján jogellenesnek minősülő **cselekményeket a társadalmi hitelrendszerben rögzítik és nyilvánosságra hozzák** (PIPL 67.).

Fontos, hogy a PIPL **olyan mechanizmust biztosít az egyének számára, amelynek keretében az adatkezelőktől kártérítést kaphatnak az általuk elszenvedett veszteségért (kárért) vagy az adatkezelő által szerzett előnyért, ha a személyes adatok kezelése sérti az egyének jogait és érdekeit** (PIPL 69.). Ha nehéz meghatározni a tényleges kárt vagy a jogellenesen szerzett hasznot, a bíróság figyelembe veheti az eset vonatkozó egyéb körülményeit. Azok az adatkezelők, akik nem tudják bizonyítani, hogy nem vétkesek az okozott kárért, felelősséggel tartoznak. Ezen túlmenően, ha az adatkezelők megtagadják az érintetti joggyakorlásra irányuló kérelmet, az bírósági jogorvoslattal élhet (PIPL 50.).

Az **egyéni igényérvényesítés lehetősége (private right of action - PRA) létezik a GDPR 82. cikkében és az Amerikai Egyesült Államok jelentős szabályozásaiban**, így szűkebb körben a kaliforniai CCPA-ben (California Consumer Privacy Act), tágabban pedig a 2023. január 1-től alkalmazandó CPRA-ben (California Privacy Rights Act).

Végül, ha a jogszabálysértés több személy jogait és érdekeit sérti, az ügyészség, valamint az érintett végrehajtó szervek is pert indíthatnak.

12. Várható következmények, gyakorlati hatások

Lényeges, hogy a vállalkozásoknak nemcsak azt kell megérteniük, mit mond a PIPL és a kínai adatvédelmi szabályozás, hanem a kínai hatóságok, vállalkozások és fogyasztók hozzáállását az adatok felhasználásához és védelméhez, valamint **a helyi végrehajtási prioritásokat is figyelembe kell venniük, amikor megfelelőségi programokat dolgoznak ki.** A PIPL azon előírása, hogy a határon túli adatkezelőknek Kína területére kifejezetten az adatvédelemért felelős képviselőt kell kinevezniük (PIPL 53.), drágítja is a megfelelőséget, nehezebb helyzetbe hozva például a kis- és középvállalkozásokat.

További **költségigényes követelmény az adatexport előtti hatásvizsgálat** (PIPL 36.), továbbá a **mennyiségi korlátozások** (PIPL 40. és 52.) – amely mennyiségek ráadásul jelenleg nem is ismertek. Megfelelési kockázatot jelent még a GDPR-ban alkalmazottakkal szinonimának tűnő, mégis kissé

eltérő jogszabályi fogalmak használata, például a már említett „controller” kifejezés helyett a „personal information handler” kifejezés használata. További bizonytalansági tényező, hogy a Kínai Kibertér Hatóság a végrehajtásért felelős szervezet, illetve egyben döntéshozó is, amely szerepet csak a gyakorlat tudja majd tartalommal feltölteni.

Az is kérdéses, **hogyan alkalmazza majd a Kínai Kibertér Hatóság azt a PIPL 43. szerinti rendelkezést, amely kölcsönös intézkedéseket tesz lehetővé bármely olyan országgal szemben, amely Kínával szemben diszkriminatív intézkedéseket fogad el**. Ez adott esetben jogalapot biztosíthat a kínai honosságú vállalkozások legnagyobb versenytársainak korlátozására is, a kínai állampolgárok adatait felhasználó nemzetközi vállalatok így a geopolitikai küzdelem célpontjaivá válhatnak.

Összefoglalva, a felsorolt kockázatok és értelmezési bizonytalanságok mellett a PIPL elvitathatatlan erénye, hogy **elősegíti jogbiztonságot és a kiszámítható üzletvitelt, hiszen rögzíti a jogalapokat és a hozzájárulás megszerzésének részletes szabályait.**

Mivel egy szakmai oldalon és fórumon vagyunk, eltekintenék az ilyenkor megjelenő tanácsadói cikkekben alkalmazott lezárástól, amely szerint már ma meg kell kezdenünk a felkészülést annak érdekében, hogy 2021. november 1-től a megfelelőség biztosított legyen, mert aki nem teszi, az nagyösszegű bírságra és további szankciókra számíthat.

Inkább adatvédelmi szakjogászként és kutatóként üdvözlöm az új jogszabályt és kíváncsian várom, milyen új hatósági és nemzetközi gyakorlatot hoz az adatvédelemben, egyben a globális színtéren pozitív – az adatvédelmi tudatosságnövelés és az egyéni érdekérvényesítés irányába tett – lépésnek tartom.

Források

- Robert Bateman: International Data Transfers Under China's Personal Information Protection Law (PIPL)

https://www.grcworldforums.com/global/international-data-transfers-under-chinas-personal-information-protection-law-pipl/2408.article

- Michelle Chan: The Gloves Are Off! China's Personal Information Protection Law was Passed and will Come into Effect on 1 November 2021

https://www.twobirds.com/en/news/articles/2021/china/chinas-personal-information-protection-law-was-passed

- China Briefing: Personal Information Protection Law in China: Technical Considerations for Companies

https://www.china-briefing.com/news/personal-information-protection-law-in-china-technical-considerations-for-companies/

- Liam Read: Analyzing China's PIPL and how it compares to the EU's GDPR

https://iapp.org/news/a/analyzing-chinas-pipl-and-how-it-compares-to-the-eus-gdpr/?mkt_tok=MTM4LUVaTS0wNDIAAAF_GCJN5GCc4fII9lebphC5qvNBuOy7wAFXAxZUvlam9fDFmtJiXl2bkCAzC3waDd9AP3Bix2xA-I0jQFTNPIv61O2LAfXY6Y46fh90_nsJflOp&utm_source=pocket_mylist

- China's New Comprehensive Data Protection Law: Context, Stated Objectives, Key Provisions

https://fpf.org/blog/chinas-new-comprehensive-data-protection-law-context-stated-objectives-key-provisions/

- Seven Major Changes in China's Finalized Personal Information Protection Law

https://digichina.stanford.edu/news/seven-major-changes-chinas-finalized-personal-information-protection-law

- eredeti szöveg:

https://zh.wikisource.org/wiki/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E4%B8%AA%E4%BA%BA%E4%BF%A1%E6%81%AF%E4%BF%9D%E6%8A%A4%E6%B3%95

- angol fordítás:

Translation: Personal Information Protection Law of the People's Republic of China (Effective Nov. 1, 2021)

https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021