Compliance és az üzleti titok

Molnár Erzsébet*

A gazdálkodó szervezetek optimális és profitorientált működéséhez elengedhetetlen, hogy olyan információkkal, adatokkal rendelkezzenek, amelyek a külvilág számára titkosak. Az ilyen adatok nyilvánosságra kerülése nem csak gazdasági hátrányt okozhat az adott szervezetnek, hanem reputációvesztéssel is járhat. A tanulmány azzal a kérdéssel foglalkozik, hogy miképpen lehet compliance eszközökkel védelemben részesíteni a gazdálkodó szervezet üzleti titkait. Ennek keretében védelmi szintek kiépítésére tesz javaslatot, valamint foglalkozik az ún. whistleblowing relevanciájával.
Kulcsszavak: *criminal compliance, üzleti titok, wistleblowing, integráció*

Compliance and trade secret
It is essential for the optimal and profit-oriented operation of business organizations to have information and data that are secret to the outsiders. Disclosure of such data may not only cause economic disadvantage to the organization, but may also result in a lost of reputation. The study deal with the question: how compliance tools can protect a business's trade secrets. In the study I propose the establishment of protection levels, as well as the study deals with the relevance of whistleblowing.
Keywords: *criminal compliance, trade secret, whistleblowing, integration*

DOI: 10.32980/MJSz.2021.1.952

1. Bevezetés

A vállalkozások, gazdálkodó szervezetek sikeres működéséhez feltétlenül szükségesek a megbízható információk, ismeretek,[1] a jogi személy léte, személyiségének érvényesülése kétségkívül nagyban függ annak gazdasági kapcsolataitól. Éppen ezért – belső integritásának, gazdasági jó hírnevének, gazdasági versenyhelyzetének megőrzése[2] – céljából egy szervezet életében jelentős szerepet játszanak a tevékenységét érintő titkok,[3] így a gazdasági, üzemi, üzleti titkok, valamint know-how megőrzése.[4] Az Európai Unió-szerte működő vállalkozások körében 2012-ben, szúrópróbaszerűen végzett reprezentatív felmérés

* Egyetemi adjunktus, Szegedi Tudományegyetem, Állam- és Jogtudományi Kar, Bűnügyi Tudományok Intézete.

[1] Wagner, Philipp: *Schutz vor Industriespionage. Analyse, Prävention und Abwehr des irregulären Verlustes von Know-how in Unternehmen*. Hamburg, Igel Verlag RWS, 2014, 1. o.

[2] Wurzer, Alexander: Know-how-Schutz als Teil des Compliance Managements. *Corporate Compliance Zeitschrift* 2009/2, 49. o.

[3] Grieger, Alexander: *Corporate Crime und Compliance. Die straf- und zivilrechtliche Verantwortlichkeit eines börsennotierten Industriekonzerns und dessen Organe für Wirtschaftsdelikte seiner Mitarbeiter*. Hamburg, Diplomica Verlag, 2010, 65. o.

[4] Törő Károly: A nem vagyoni kártérítés gyakorlati kérdései. *Magyar Jog* 1992/8, 452. o., in.: Görög Márta: *A know-how jogi védelmének alapvető kérdései.* HVG Orac, Budapest, 2012, 11. o.

alapján, a megkérdezett 537 vállalkozás képviselőinek 75%-a nyilatkozott akképpen, hogy az üzleti (üzemi) titok jelentős stratégiai szerepet játszik a szervezet növekedése (fejlődése), versenyképessége, valamint alkotóképessége, innovatív teljesítőképessége terén.[5] Nem kétséges tehát, hogy ezen belső információk illetéktelen személy tudomására jutása, jogosulatlanul történő megszerzése a szervezet további létét hátrányosan befolyásolhatja, ugyanis ezen információk „elvesztését" követően nincsen mód az azt megelőző állapothoz való visszatérésre.[6] Nem véletlen tehát, hogy az üzleti titok védelmét számos jogterület biztosítja, a védelem tehát szerteágazó és interdiszciplináris: vizsgálható polgári jogi, munkajogi,[7] versenyjogi, illetve – az ultima ratio elvének szem előtt tartásával – annak büntetőjogi aspektusa. Az üzleti titok generális védelmét biztosítja 2018. július 31-i hatályba lépése óta az üzleti titok védelméről szóló 2018. évi LIV. törvény. Jelen tanulmány célja annak vizsgálata, miképpen biztosítható az üzleti titok védelme a gazdálkodó szervezeten, vállalkozáson belül, azaz miképpen előzhető meg az üzleti titok, az ún. vállalati titok[8] *rendellenes* elvesztése. A szervezetnek elődleges érdeke az, hogy a tevékenységét érintő titkát megtartsa, illetéktelenektől megóvja, ennek megfelelően a bűncselekmény, jogellenes cselekmény elkövetésének megelőzését szolgáló, preventív szervezeti intézkedési mechanizmusok léte az üzleti titok megőrzésének elsődleges eszköze.

A vállalati titok védelmét biztosító, szervezeti szabályok, védelmi mechanizmusok megfogalmazásához szükséges az ún. *compliance* fogalom meghatározása, ugyanis a vállalati titok szervezeti védelmét szolgáló intézkedések és rendelkezések összességének rendszerbeli helyének meghatározása fontos előkérdés. *(II. rész)*

A vállalkozások gazdasági, piaci létét pozitíve meghatározó ismeretek megőrzését szolgáló védelmi mechanizmusok telepítése azonban nem csak az ismeretek, tények, adatok illetéktelen személyek tudomására jutását megakadályozni hivatott intézkedések halmaza, hanem az ismeret *titok* jellegét determináló követelmény is egyben.[9] Ennek megfelelően esszenciális érdek annak meghatározása, milyen

---

[5] Az Európai Parlament és a Tanács irányelve a nem nyilvános know-how és üzleti információk (üzleti titkok) jogosulatlan megszerzésével, felhasználásával és felfedésével szembeni védelemről. 2013/042. https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX%3A52013PC0813 (*továbbiakban*: Know-how irányelv)

[6] Know-how irányelv, 15. o.

[7] A munka törvényéről szóló 2012. évi I. törvény 8. § (4) bekezdése rendelkezik az üzleti titok megőrzésének kötelezettségéről, azzal, hogy kimondja: *„A munkavállaló köteles a munkája során tudomására jutott üzleti titkot megőrizni."* Az üzleti titok munkajogi védelméről lásd. Cséffán József: *A munka törvénykönyve és magyarázata*. Szeged, Szegedi Rendezvényszervező Kft, 2014, A know-how védelmét biztosító munkajogi szabályozásokról lásd: Görög: i.m. 81-83. o.

[8] Vállalati titok alatt – jelen tanulmány keretei között – értendő minden olyan titok [különösen üzleti (üzemi) titok, valamint know-how], amely titok léte és megőrzése szervezeti érdek, és a megőrzésüket szervezeti intézkedések biztosítják. Jelen tanulmányban a vállalati titkok terminológiát az üzleti titok fogalom szinonimájaként használom, az üzleti titok szervezeti, vállalati jellegzetességeinek hangsúlyozása céljából. A terminus szervezeti jogban, gyűjtőfogalomként való használata létjogosultságához lásd. Frank, Torben: *Der Schutz von Unternehmensgeheimnissen im öffentlichen Recht*. Freiburg, Peter Lang Verlag, 2008, 20. o, 38. o, Stadler, Astrid: *Der Schutz des Unternehmensgeheimnisses im deutschen und U.S.-amerikanischen Zivilprozess und im Rechtshilfeverfahren*. Tübingen, J. C. B. Mohr, 1989, 6-7. o.

[9] TRIPS Egyezmény 39. Cikk 2. pontja.

intézkedések foganatosítása elégséges ahhoz, hogy egy ismeret, tény, adat egyáltalán *titoknak* minősüljön, mindemellett pedig szükséges azon potenciális veszélyforrásoknak a felismerése és definiálása, amelyek a védelmi igény alapjául szolgálnak. *(III. rész)*

A vezető tisztségviselő a szervezet részét képező azon személy, aki tipikusan abban a tény- és joghelyzetben van, hogy a szervezet munkavállalóinak, tagjainak, dolgozóinak magatartását ellenőrizni, felügyelni képes, és köteles is egyben. Éppen ezért abban az esetben, ha a szervezet valamely tagja bűncselekményt követ el, úgy vizsgálandó a vezető tisztségviselő büntetőjogi felelőssége fennállásának kérdése is. *(IV. rész)*

A szervezet tevékenységét érintő titkok megőrzéséhez fűződő érdek méltányolható *szervezeti magánérdek*, nem élvez azonban abszolút, korlátozhatatlan védelmet, amely azt jelenti, hogy valamely vállalati titok megsértésének jogellenességét kizáró okok hatályosulhatnak,[10] amely körülmény azonban a szervezetnek – jogellenesség (üzleti titok vonatkozásában adott esetben bűncselekmény megvalósulásának, büntető-jogellenesség) hiányában is – objektív sérelmet okozhat. Éppen ezért a szervezet érdeke a titok bármilyen áron történő megtartása. Az üzleti titok nyilvánosságra hozatalának elkerülésére szolgáló megfelelő eszköz lehet az ún. internal whistleblowing intézménye. *(V. rész)*

2. A compliance jelentése és releváns alkalmazási területei

A vállalkozások életében számos olyan kockázati tényező merül fel, amelyek eliminálása, minimalizálása elemi szervezeti érdek. E kockázati tényezők közül az egyik legjelentősebb a szervezet versenyhelyzetének, gazdasági versenyben betöltött kedvező pozíciójának, ill. reputációjának potenciális elvesztése.[11] Éppen ezért egy vállalkozás, gazdálkodó szervezet életében elengedhetetlen olyan intézkedés- és szabályrendszer, ill. felügyeleti rendszer kiépítése, amely belső integritásának védelmét szolgálja azzal, hogy nem csak a gazdasági, hanem a jogi kockázatokat (amelyek persze végső soron tipikusan gazdaságban realizálódó következménnyel bírnak) is igyekszik előre feltárni, majd megelőzni,[12] ill. minimalizálni.[13] E cél megvalósításának eszköze az ún. *compliance*. Az angol eredetű compliance terminus szószerinti jelentése *betartás, egyetértés, követés*.[14] A fogalom eredetileg az orvostudományból származik, ahol is a beteg terápiakövető

[10] Frank: i.m. 44. o.

[11] Zenke, Ines – Schafer, Ralf – Brocke, Holger: *Risikomanagement, Organisation, Compliance für Unternehmer*, Berlin, Walter de Gruyter GmbH, 2015, 53. o.; Vö. Ambrus István-Farkas Ádám: *A compliance alapkérdései. Az etikus vállalati működés elmélete és gyakorlata.* Budapest, Wolters Kluwer, 2019, 20. o.

[12] Ambrus-Farkas i.m. 20. o.

[13] Rotsch, Thomas: Criminal Compliance – Begriff, Entwicklung und theoretische Grundlegung, in. *Criminal Compliance* (szerk.: Rotsch, Thomas), Baden-Baden, Nomos, 2015, 31-81. 39. o.

[14] Jacsó Judit: A compliance fogalmáról és szerepéről a gazdasági életben, *Miskolci Jogi Szemle* 2019/1, 82-91. 83. o.

magatartását jelenti.[15] A jogi fogalomkészletbe való átvételére az orvostudományban használatos fogalomra vont analógiával került sor, mégpedig *„to be compliance with the law"*[16] értelemben, ennek megfelelően a fogalom alapvetően az érvényes és hatályos jogi normákkal egyetértésben való cselekvést jelenti.[17] A *compliance* definíciószerűen mindazon intézkedések összessége, amelyek megtételét megköveteljük a vállalkozásoktól annak érdekében, hogy garantáljuk: a vállalkozások, illetőleg azok tagjai és dolgozói minden jogi- illetve etikai norma által előírt kötelezettséget teljesítsenek, a tilalmakra vonatkozó szabályokat pedig betartsák.[18] Azaz a compliance egyfajta szervezeten belüli normakonformitás,[19] legyen szó akár jogi, akár szervezeti etikai szabályrendszerről. A compliance intézkedésorientált aspektusa a normakövetést biztosítását szolgáló intézkedések, eljárások összessége,[20] amelyek lehetnek normatív, intézményi, valamint technikai jellegűek.[21] Mindezen említett, az intézkedésorientált compliance aspektus alá sorolható intézkedéseket rendszerbe foglaló intézmény a compliance szakirodalom által definiált, ún. *compliance management rendszer* (Compliance Management System – *CMS*).[22] A CMS szerves részét képezi a rizikómanagement, amely célja a gazdasági kockázatok idejekorán történő felismerése, analizálása és értékelése annak érdekében, hogy a szükséges intézkedések meghozásával ezek a kockázatok minimalizálhatók, eliminálhatók legyenek.[23] Kocziszky-Kardkovács szerzőpáros megfogalmazása szerint a CSM *„azoknak a tevékenységeknek a tudatos rendszerbe foglalása, amelyek eredményeként az adott gazdálkodó szervezet munkavállalói ismerik a feladataik ellátásához kapcsolódó jogszabályi, etikai, szakmai és teljesítmény-előírásokat, elvárásokat, valamint az előírásoktól, elvárásoktól való eltérésre (beépített) kontrollok figyelmeztetnek, illetve a kontrollok segítségével a rendszer korrekciós lehetőségeket ajánl fel, így a szervezet felkészülhet a problémák kezelésére, kijavítására."*[24]

A compliance-nek számos aspektusa definiálható, választható el egymástól in thesi[25] attól függően, hogy az adott szervezetre vonatkozó norma, intézkedés, mely

---

[15] Vö. *uo*. 83. o.

[16] Rotsch, Thomas: Criminal Compliance. *Zeitschrift für Internationale Strafrechtsdogmatik* 10/2010, 614. o.

[17] Rotsch: *Criminal Compliance – Begriff, Entwicklung und theoretische Grundlegung* 39. o.

[18] Reichert, Jochem: Reaktion pflichten und Reaktionsmöglichkeiten der Organe auf (möglicherweise) strafrechtsrelevantes Verhalten innerhalb des Unternehmens, *Zeitschrift für Internationale Strafrechtsdogmatik*. 3/2011, 114. o.

[19] Rotsch: *Criminal Compliance – Begriff, Entwicklung und theoretische Grundlegung* 40. o.

[20] Bock, Dennis: Strafrechtliche Aspekte der Compliance-Diskussion - § 130 OWiG als zentrale Norm der Criminal Compliance, *Zeitschrift für Internationale Strafrechtsdogmatik* 2/2009, 68-81. 68. o.

[21] Így pl. normatív compliance intézkedésnek tekinthető a szervezeten belül etikai kódex létrehozása, intézményi jellegű compliance officer pozíció integrálása a szervezetrendszerbe, valamint technikai jellegű pl. szervezeten belüli whistleblower-hotline kiépítése. Lásd: Rotsch: *Criminal Compliance – Begriff, Entwicklung und theoretische Grundlegung* 41. o.

[22] *Uo.* 41. o., vö. Jacsó: i.m. 83. o.

[23] Zenke–Schafer–Brocke: i.m. 2. o.

[24] Kocziszky György – Kardkovács Kolos: A compliance szerepe a közösségi értékek és érdekek védelmében. Elmélet és gyakorlat. Budapest, Akadémiai Kiadó, 2020. 96. o.

[25] A fogalmi elhatárolás – tipikusan compliance-criminal compliance relációban – elméletinek tekinthető annyiban, hogy a gyakorlatban nehéz megtalálni azt a határt, amikor is az intézkedés kifejezetten

jogterülethez kapcsolódó *jogkövetést* szolgál.[26] Ennek megfelelően a compliance-nek van büntetőjogi aspektusa is, amelyet a szakirodalom criminal compliance-ként definiál. A criminal compliance kifejezetten a büntetőjogilag releváns cselekményekre koncentráló terminus technicus, amelynek tárgya egyrészről – a compliance-fogalom analógiájára – büntetőjogi normák betartása,[27] azaz bűncselekmények elkövetésétől való tartózkodás, másrészről büntetőjogilag releváns magatartások előfordulását minimalizálni törekvő, illetve büntetőjogi felelősségre vonást elkerülését célzó intézkedések foganatosítása, e célok elérését szolgáló rendszer kiépítésének követelménye a szervezeten belül.[28]

A CMS, különösen a rizikómanagement, általánosan fontos a szervezet materiális és immateriális gazdasági erőforrásainak optimális kihasználása érdekében, ugyanis a profitorientált szervezet célja tipikusan a nyereség maximalizálása.[29] Éppen olyan fontos azonban a jogi – éspedig különösen a büntetőjogi – kockázatok felismerése, értékelése, és azok minimalizálására, eliminálására adekvát rendszer kiépítése. Bűncselekmény, jogellenes cselekmény szervezeten belüli elkövetése potenciális lehetőségének felismerése engedhetetlen feltétele a megfelelő és hatóképes CMS kiépítésének, ugyanis felismerés, előrelátás nélkül aligha lehetséges hatékony intézkedések foganatosítása a veszély elkerülése érdekében.[30]

3. Titokvédelmi rendszer kiépítésének követelménye és a releváns kockázati tényezők

A kutatás-fejlesztés (K+F) a technológiai fejlődés egyik alapköve, a technológiai fejlődés pedig a gazdasági növekedés egyik mozgatórugója.[31] Az ismeretek optimális fel- és kihasználása érdekében a vállalkozásnak mérlegelnie kell: a tudás, az információ, amely birtokában van, olyan versenyelőnyt jelent számára, amely előny annak titokban tartásával biztosítható legoptimálisabb módon, avagy a rendelkezésére álló ismeretet egyéb jogi védelemben kívánja részesíteni, ezzel a titkosságból származó tényleges vagy potenciális előnyökről lemondva meghatározott időre szóló, egyéb jogi védelem eszközeit élvezi. Bármely lehetőség melletti döntés gondos mérlegelést igényel. Látható, hogy a titokban tartás optimális gazdasági versenyhelyzetet teremt a szervezet számára, látni kell azonban azt is, hogy jelentős kockázatot hordoz magában. A szervezeten belül az ún. titok-rizikó (know-how-rizikó[32]) egy olyan kockázati faktor,[33] amely speciális védelmi

büntetőjogi értelemben vett preventív hatás kiváltását hivatott szolgálni, ennek megfelelően vegytiszta criminal compliance intézkedésekről praxisorientált értelemben tulajdonképpen nem beszélhetünk. ROTSCH *Criminal Compliance – Begriff, Entwicklung und theoretische Grundlegung* 36. o.

[26] A compliance hatókörével kapcsolatban lásd: Ambrus-Farkas i.m. 46-47. o.

[27] *Uo*. 41. o.

[28] *Uo*.

[29] *Uo*. 42. o.

[30] *Uo*. 44. o.

[31] Grieger: i.m. 65. o.

[32] Wurzer: i.m. 52. o.

[33] Grieger: i.m. 65. o.

mechanizmusok gondos kiépítését igényli annak érdekében, hogy a szervezet megóvja önmagát a vállalati titok potenciális elvesztésével járó hátrányos gazdasági következményektől.[34] E kockázat általában véve az ismeret, a tapasztalat, az adat titok jellege megszűnésének potenciális lehetősége[35] azáltal, hogy az illetéktelen személy birtokába kerül, illetve a titokkal rendelkezni jogosult személy rendelkező cselekménye hiányában válik quasi közkinccsé. A vállalkozást érintő titkok léte, létének pozitív hatása nem újkeletű jelenség, azonban a technika fejlődése természetszerűleg nehezíti meg a szervezet versenyképességét elősegítő, adott esetben profitját megalapozó ismeretek, adatok megőrzését.[36] Ezért annak érdekében, hogy a vállalkozás számára fontos ismeretek – döntésétől függően – titoknak minősüljenek, ill. a titok a szervezet keretei között maradva az arra jogosult rendelkezésének hiányában ne kerülhessen a szervezeten kívülre, adekvát védelmi rendszer kiépítése szükséges. Ehhez – mint láthattuk – első lépés a veszély, a kockázat felismerése, definiálása, majd a felismerésnek megfelelően adekvát CMS kiépítése.[37] Az alábbiakban a vállalati titokra vonatkozó releváns kockázatok, illetve a titokjellegből eredő implicit követelmények absztrakt felvázolása mentén, horizontális, valamint vertikális aspektusban egy optimális védelmi rendszer kiépítése ismérveinek vázolására vállalkozok.

3.1. A védelem szintjei. A védelem szintjei alatt a titokvédelmi rendszer vertikális realizálása értendő. Fontos, hogy egy adat, ismeret, információ, tapasztalat önmagában attól, hogy az unikális jellegű, még nem minősül titoknak, a titokjelleg fennállásában a fogalmi kritériumok alapján történő állásfoglalás a bíróság feladata.[38] Ennek megfelelően a titokvédelem első (quasi nulladik) szintjének tekintendő mindazon – minimális – rendelkezések és intézkedések összessége, amelyek az ismeret, adat *titokká minősüléséhez* szükségesek.[39] Az üzleti titok körébe tartozó titokkal kapcsolatos védelmi igény e titokfajták fogalmából explicite következő kritérium.[40] Ugyanis a TRIPS Egyezmény 39. Cikke akképpen rendelkezik, hogy az ismeret abban az esetben minősül egyáltalán titoknak (egyéb kritériumok fennállása mellett), ha *„titokban tartása érdekében az adatok felett ellenőrzés gyakorlására feljogosított személy a körülményekhez képest ésszerű lépést tett.”*[41] E kritérium az Üttv. által definiált üzleti titok fogalmában explicite is megjelenik azzal, hogy a jogalkotó akképpen rendelkezik, hogy az üzleti titok védelmére vonatkozó

[34] Az üzleti titok megsértése bűncselekményt *Ambrus-Farkas* szerzőpáros is tipikus vállalati visszaélésként megjelenő deliktumként tipizálja. Ambrus-Farkas: i.m. 115. o.

[35] Frank: i.m. 39. o.

[36] Vö. Sántha Ferenc: Az üzleti titok büntetőjogi védelme a nemzetközi jogfejlődés tükrében. *Miskolci Jogi Szemle* 2019/1. 42-64. 42. o.

[37] Dolota, Uwe: *Compliance contra Wirtschaftskriminalität. Korruption im Wandel der Zeit.* Hamburg, Disserta Verlag, 2014, 53. o.; Optimális CSM kiépítésének lépéseihez, folyamatához lásd részletesen: Kocziszky-Kardkovács i. m. 159-214. o.

[38] Sántha: i.m. 47. o.

[39] Ilyen alapvető intézkedésnek minősülhet pl. az ismeret, adat, tény titok jellegének rögzítése munkaszerződésben, avagy munkavégzésre irányuló egyéb jogviszonyt keletkeztető szerződésben

[40] Az üzleti titoknak minősülés fogalmi kritériumainak részletes elemzését lásd: *uo.* 45-48. o.

[41] Az Általános Vám- és Kereskedelmi Egyezmény (GATT) keretében kialakított, a Kereskedelmi Világszervezetet létrehozó Marrakesh-i Egyezmény és mellékleteinek kihirdetéséről szóló 1998.évi IX. törvény C) Melléklet. Lásd. Görög: i.m. 33. o.

szabályok akkor relevánsak, ha *a titokban tartása érdekében a titok jogosultja az adott helyzetben általában elvárható magatartást tanúsítja*."[42] A következő védelmi szint azon intézkedések foganatosítása, amelyek minél magasabb szinten szolgálják a titok szervezeten belül maradását, a szervezet belső integritásának minél optimálisabb kihasználása a titokvédelem érdekében.[43]

A vállalati titok fogalmi körébe tartozó üzleti titok, valamint know-how védelmi szint tárgyalása vonatkozásában történő különválasztása relevanciával bír, ugyanis addig, amíg az ténytitok, azaz az üzleti titok *titoknak* minősülése esetén abszolút védelmet élvez, a know-how, azaz az ismerettitok védelme pusztán relatív. E relativitás abban áll, hogy abban az esetben, ha az ismeretre valaki az Üttv.-ben taxatíve meghatározott magatartások, tevékenységek útján tesz szert, úgy a know-how „megszerzése" nem minősül titoksértésnek.[44] A know-how magánjogi védelmének relativitása compliance szempontból annyiban releváns, hogy e relativitás a védelmet megnehezíti, illetőleg a relativitásra okot adó független fejlesztés, valamint műszaki visszafejtés ellen tulajdonképpen lehetetlen védekezni.

3.2. A védelem frontjai. A vállalati titok horizontális védelmét három fronton kell megteremteni. Az első front a szervezeten belüli munkavállalók, tagok, illetve dolgozók (insider)[45] releváns magatartásai, a második front a szervezet, vállalkozás részét nem képező, attól független, extraneus személyek cselekményei, a harmadik font pedig azon személyek köre, akik korábban a szervezet részét képezték, azonban annak elhagyásával de facto extraneussá váltak. Az optimális CMS kiépítése érdekében mindenekelőtt a potenciális veszély említett irányainak felismerése szükséges. Ugyanis a vállalati titok védelmére nem csak külső, illetéktelen személy általi „támadás" jelent veszélyt, épp oly rizikófaktort képeznek a szervezet munkavállalói, egykori munkavállalói, tehát azok a személyek, akik jogszerűen vannak az adott ismeret birtokában. A szervezeten belül dolgozó személyek mint veszélyforrások szintén két irányból definiálhatók, mégpedig azon ismérv mentén, hogy a cselekményük a szervezet *érdekét* szolgálja,[46] avagy az a szervezetet károsítja. A két aspektust a német szakirodalom két különböző terminussal illeti: amíg az első esetkörbe tartozó bűncselekmények elkövetése körét *Entlastungskriminaliät* fogalommal illeti, addig a második esetkörben ún. *Belastungskriminalität*-ről van szó.[47] Mindkét fogalom szervezeti relevanciában használatos, amely azt jelenti, hogy e nézőpontból e fogalmi kategóriák alá eső

[42] Üttv. 1. § (1) bekezdés

[43] Így pl. különböző technikai jellegű, IT védelmi rendszerek, versenytilalmi, ill. titokvédelmi megállapodások.

[44] Az Üttv. 5. § (1) bekezdésben megfogalmazott kivételek alapján nem minősül know-how megsértésének, ha valaki független fejlesztés, vagy ún. műszaki visszafejtés révén jutott az ismeret birtokába [a) pont]. Vö. Faludi Gábor: Az üzleti titokhoz való jog. Know-how. (Ptk. 2:47.§), in. *A polgári törvénykönyv magyarázata* (szerk.: Vékás Lajos), Budapest, Complex 2013, 60. o.

[45] Jelen tanulmány keretei között insider személy a vállalkozás, gazdálkodó szervezet tagja, vagy dolgozója, azaz a szervezet részét képező személy.

[46] Tipikusan korrupciós bűncselekmények sorolhatók e fogalmi kategória alá.

[47] Bock, Dennis: Stand der strafrechtswissentschaftlichen Compliance-Diskussion in Deutschland, in: *Wissenschaftliche und praktische Aspekte der nationalen und internationalen Compliance-Diskussion* (szerk.: Thomas Rotsch), Baden-Baden, Nomos Verlagsgesellschaft, 2012, 63-76. 64. o.

bűncselekmények elkövetője kizárólag insider személy lehet. Amennyiben az insider az üzleti titok[48] megsértésének bűncselekményét[49] azon szervezethez tartozó titokra követi el, amely őt foglalkoztatja, úgy a bűncselekmény természetszerűleg a szervezet ellen irányul, a szervezetet károsítja. A Btk. az üzleti titok megsértésének tényállását közönséges bűncselekményként fogalmazza meg, azaz elkövetők tekintetében nem differenciál, azt bárki, így akár insider, akár extraneus elkövetheti.[50]

Kockázati szempontból a vállalati titokra talán a gazdálkodó szervezetet elhagyó ex-tagok, ill. dolgozók jelentik a legnagyobb veszélyt. E probléma különösen a munkavállalói fluktuáció[51] mértékére tekintettel válik igazán hangsúlyossá. Ugyanis a szervezet által védett adatok, ismertek birtokában jogszerűen lévő munkavállalók gyors fluktuálódása[52] azt a logikus következményt vonja maga után, hogy az általuk ismert titok a szervezeten kívülre kerül, és ezáltal fennáll a veszélye annak, hogy az ismeretet a munkavállaló könnyen más, hasonló profilú vállalkozás tevékenységének elősegítése érdekében kamatoztatja.

A leghatékonyabb védelmi rendszer az insider cselekményeivel szemben építhető ki, ugyanis a szervezet részét képező személy a szervezeti CMS normatív eszközrendszerének hatálya alatt áll, jogellenes magatartása esetére a szankcióval való fenyegetettség már a szervezeten belül, belső eszközrendszer alkalmazásával adott. Az extraneus személy jogellenes magatartásával szembeni védekezésre az iménti személyi körtől eltérően természetszerűleg korlátozottabb lehetőségek állnak rendelkezésre. E vonatkozásban tipikusan a CMS technikai aspektusa jöhet szóba. Jelen tanulmánynak nem célja a CMS technikai aspektusának részletes vizsgálata és ilyen jellegű megoldási javaslatok felvázolása, ugyanakkor e témakör különös figyelmet érdemel azért, mert – ahogyan azt *Sántha* megfogalmazza – *„a kibertér infokommunikációs technológiáinak alkalmazása […] lehetővé teszik a versenytársak, a céges alkalmazottak, vagy akár külföldi titkosszolgálatok számára is, hogy gyorsan és észrevétlenül ellopjanak és továbbítsanak óriási mennyiségű adatot”.*[53] A végeláthatatlan technikai fejlődés adta lehetőségek tehát az elkövető szervezethez fűződő viszonyától függetlenül óriási kihívások elé állítják a titok jogosultját. E támadásokkal szembeni jogi alapokon nyugvó technológiai védekezés minden szervezet CMS rendszerének részét kell képeznie.

A vállalati titokra legveszélyesebb kockázati front a szervezetet elhagyó munkavállaló. Ugyanis a de facto extraneus személy tipikusan jogszerűen van a

[48] A vállalati titok fogalom alól e helyen az üzleti titok következetesen kerül kiragadásra, ugyanis a hatályos magyar jogi szabályozás keretei között a vállalati titok gyűjtőfogalom alá értendő know-how nem élvez büntetőjogi védelmet. Azaz büntetőjogilag releváns kérdések vizsgálata során a fogalmak egymástól elválasztandók.

[49] A Büntető Törvénykönyvről szóló 2012. évi C. törvény (Btk.) 418. §

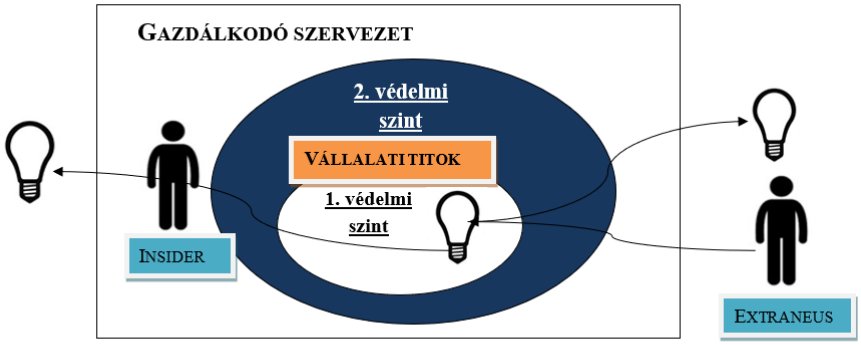
[50] Vö. Sántha: i.m. 54. o. Formailag ettől eltérő szabályozással találkozhatunk a német jogrendszerben, ugyanis a tisztességtelen versenyről szóló törvény *(Gesetz gegen unerlaubte Wettbewerb)* egymástól eltérő elkövetési magatartások realizálása esetén, külön fordulatban rendeli büntetni az insider, illetve az extraneus személyt. *(UWG § 17 Verrat von Geschäfts- und Betriebsgeheimnissen)*

[51] A munkavállalói fluktuáció mint CMS szempontjából releváns rizikóhoz lásd: Kocziszky-Kardkovács: i. m. 208. o.

[52] Grieger: i.m. 65. o.

[53] Sántha: i.m. 43. o.

védeni kívánt titok birtokában, azonban nem képezi már a szervezet részét, adott esetben a szervezethez való lojalitás nem áll többé érdekében, ad absurdum de facto károkozási szándéka realizálásához a legoptimálisabb helyzetben van a titok továbbadása lehetőségével a kezében. E tekintetben úgy a technikai eszközök általi titokvédelem, mint az insiderre vonatkozó belső normatív szabályok léte irreleváns védelmi eszköz. E valóban potenciális veszélyforrás elleni védelem megfelelő eszköze lehet az, ha a de facto extraneus személyt – preventíve – *de jure intraneussá* teszi a szervezet. Azaz a vállalkozásból történő kilépéskor jogi eszközzel kell gondoskodni arról, hogy a vállalati titokkal kapcsolatban jogellenes cselekmény elkövetésétől visszariadjon. A versenytilalmi megállapodás tipikusan e célt szolgáló magánjogi eszköz.



(1. ábra)

4. A vállalkozás vezetőjének üzleti titok megsértéséért fennálló büntetőjogi felelősségének kérdése

Az üzleti titok megsértése a vállalkozás érdekeit sértő bűncselekmény. Kriminológiai szempontból e kijelentést árnyalni kell azonban. Ugyanis abban az esetben, ha valamely vállalkozás tagja vagy dolgozója egy másik szervezet üzleti titkát azért szerzi meg jogosulatlanul, hogy a megszerzett adatot, ismeretet az őt foglalkoztató szervezet javára fordítsa, úgy a bűncselekmény elkövetése e másik szervezet relevanciájában tulajdonképpen *szervezeti érdek*. Azaz addig, amíg a titok jogosultjaként megjelenő vállalkozás hátrányt szenved, addig egy másik vállalkozáshoz tartozó, e szervezet vonatkozásában insider személy által elkövetett bűncselekmény e szervezet oldalán előnyként jelenik meg. Abban az esetben, ha a szervezet tagja vagy dolgozója az üzleti titok megsértésének bűncselekményét a szervezet javára, annak érdekében követi el, úgy felmerül az előnyt potenciálisan élvező szervezet vezetője büntetőjogi felelősségének kérdése is.

A szervezet vezetőjének büntetőjogi felelőssége a lehetséges elkövetői alakzatok bármelyike alapján fennállhat. Az elkövetői alakzatok közül jelen fejezet keretei között azonban pusztán a mulasztásos bűnsegély dogmatikai kategóriájával foglalkozom.

A szervezet tagjai, dolgozói bűncselekmény, jogellenes cselekmény potenciális elkövetésének vonatkozásában quasi veszélyforrásként definiálhatók,[54] éspedig annak megakadályozása, hogy e veszélyforrás tényleges sérelmet realizáljon, tipikusan a szervezet vezetőjének általános felügyeleti és ellenőrzési kötelezettségéből származó felelőssége, ugyanis a szervezet hierarchikus szervezettsége okán e veszélyforrás „kordában tartására" szolgáló, tipikusan jogi eszközök rendelkezésére állnak. Amennyiben a vezető tisztségviselő ezen felügyeleti-ellenőrzési kötelezettségének teljesítését annak érdekében, vagy abba belenyugodva mulasztja el, hogy azzal lehetővé tegye a bűncselekmény elkövetésének megvalósulását, úgy az üzleti titok megsértéséért bűnsegédként fennálló felelőssége vizsgálatának kérdése releváns.[55] Ugyanis amennyiben elfogadjuk a mulasztásért fennálló felelősség alapjául szolgáló speciális jogi kötelezettségek létét,[56] úgy a vezető tisztségviselőt speciális jogi kötelezettség terhelheti harmadik személy magatartásáért fennálló felelősség okán.[57] Amennyiben pedig cselekvési lehetőség és képesség ellenére elmulasztja megakadályozni azt, hogy a felelősségi (felügyeleti-ellenőrzési) körébe tartozó személy bűncselekményt kövessen el, úgy a vezető tisztségviselő büntetőjogi felelőssége mulasztásos bűnsegély dogmatikai kategória alapján áll fenn.[58]

5. A vállalati titok védelme internal whistleblowing útján – Védelem a nyilvánosságra hozás ellen nyilvánosságra hozással?

Mivelhogy a gazdálkodó szervezet (egykori) tagjai, dolgozói jelentős potenciális veszélyforrást jelentenek a vállalati titokra nézve, úgy e veszélyforrásban rejlő kockázatot minimalizálni, illetve eliminálni kell. Ugyanis az üzleti titok szervezeten kívülre kerülésének káros hatását nem befolyásolja az a kérdés: vajon az elkövető tényállásszerű magatartása egyben jogellenes is volt-e. A probléma vizsgálatának, valamint adekvát megoldási javaslat kidolgozásának igényét az az uralkodó szakirodalmi álláspont adja, miszerint "*nem minősíthető a közlési tilalom, illetve titoktartási kötelezettség megszegésének, ha pl. a munkavállaló a munkája során*

[54] Mittelsdorf, Kathleen: Zur Reichweite individueller strafrechtliche Verantwortung im Unternehmen für Fehlverhalten von unterstellten Mitarbeitern. *Zeitschrift für Internationale Strafrechtsdogmatik* 2011/3, 123-128, 126. o.

[55] Mulasztásos bűnsegélyért való felelősség megállapítására a gyakorlatban viszonylag ritkán kerül sor, hiszen a mulasztás ontológiai kritériumainak bizonyítása rendkívül nehéz.

[56] Lásd részletesen: Molnár Erzsébet: Büntetőjogi felelősség a magánjogiasodás útján? A mulasztás büntetendőségének normatív alapjáról a vezetői felelősség tükrében. *Forum Acta Juridica et Politica* 2019/2, 83-112, 89-108. o.

[57] Nagy Ferenc: *Anyagi büntetőjog. Általános rész,* Szeged, I. Iurisperitus Bt, 2013, 167. o.

[58] Mulasztásos bűnsegélyről akkor beszélünk, ha „az a személy, akit a más által elkövetett bűncselekmény megakadályozására nézve speciális jogi kötelezettség terhel, ennek ellenére nem tesz meg minden tőle telhetőt a megakadályozás érdekében." Nagy: i.m. 351. o.

tudomására jutott bűncselekmény felderítése érdekében – közérdekű bejelentés formájában, vagy a büntető hatóság előtti meghallgatása során – hivatkozik az üzemi (üzleti) titokra."[59] A védelmi cél eléréséhez több szempontból is alkalmasnak minősülhet egy, a szervezeten belül kiépített, azaz ún. internal whistleblowing rendszer.

5.1. A whistleblowing jelentése[60] Az angol eredetű *whistleblowing* kifejezés jogi értelemben[61] – legtágabban – valamiféle jogsértés, normasértés *nyilvánosságra hozását* jelenti. Szűkebb értelemben[62] a gazdálkodó szervezeten belül, illetve a szervezet tevékenységével összefüggésben elkövetett jogsértések nyilvánosságra hozását értjük alatta.[63] Habár a jogtudományban nincsen egyetlen, kizárólagosan elfogadott whistleblowing fogalom,[64] az egyes lényes fogalmi elemek ismeretében definiálható, mit is értünk valójában alatta. Ekképpen *whistleblower* az a vállalkozás részét képező, azon belül tevékenykedő személy, aki a szervezeten belül észlelt jogsértéseket – legyen szó akár bűncselekményről, akár más jogági vagy etikai normasértésről[65] – meghatározott szervnek vagy személynek, a szervezeten belül, vagy azon kívül jelenti, annak érdekében, hogy az megfelelő módon orvoslásra kerüljön.[66] Az *International Handbuch on Whistleblowing Research* szerzői a következőképpen definiálják a whistleblower személyét: *„a whistleblower alapvetően szervezeti vagy intézményi bennfentes, aki az adott szervezeten belüli vagy a szervezet által megvalósított jogsértést valaki másnak elárulja, azzal a szándékkal, vagy azzal a hatással, hogy a jogsértés orvoslása érdekében intézkedés történik"*.[67] Látható tehát, hogy a whistleblowing-nak lényeges fogalmi eleme a compliance immanens célja, miszerint a fennálló jogsértést meg kell szüntetni, orvosolni kell.

A Transparency International Hungary magyar kontextusban a *közérdekű bejelentő* fogalom használatát tekinti irányadónak.[68] Vitathatatlan, hogy egy

[59] Cséffán: i.m. 32. o.

[60] Whistleblowing jelentésével kapcsolatban lásd részletesen: Molnár Erzsébet: A közérdekű bejelentés bűnmegelőzési és bűnfelderítési relevanciájának vizsgálata a gazdálkodó szervezeten belül elkövetett bűncselekmények vonatkozásában, *Belügyi Szemle* 2016/9, 76-100, 80-83. o., vö. Ambrus-Farkas: i.m. 127-128. o.

[61] A kifejezés szó szerinti jelentése sípfúvás, metaforikus értelemben jelenti a vészharangok megkongatását. (Lásd: Abraham, Jens: Whistleblowing – Neue Chance für eine Kurswendel!? *ZRP* 2012/11, 1. o.)

[62] A fogalom, a jelenség szűkebb értelemben történő meghatározására *compliance relációban* kerül sor, ugyanis a whistleblowing tipikusan a gazdálkodó szervezet CMS-ének részét képező, visszaélés-felderítési aspektusból releváns eszköz, intézményrendszer.

[63] Rotsch, Thomas-Wagner, Markus: Whistleblowing, in. *Criminal Compliance* (szerk.: Rotsch, Thomas), Baden-Baden, Nomos, 2015, 1308-1353, 1314. o.

[64] Böckler, Hans: *Whistleblowing*, Düsseldorf, Setzkasten GmbH, 2011, 6. o.

[65] Hefendehl, Roland: Alle lieben Whistleblowing, in. *Grundlagen des Straf- und Strafverfahrensrecht. Festschrift für Knut Amelung zum 70. Geburtstag* (szerk.: Martin Böse-Detlev Sternberg-Lieben), Berlin, Dunckler & Humbolt, 2009, 618. o.

[66] Böckler: i.m. 6. o.

[67] Lewis, David – Brown, A. J. – Moberly, Richard: Whistleblowing, its importance and the state of research. in. Brown, A. J. – Lewis, David – Moberly, Richard – Vandekerckhove, Wim: *International Handbuch on Whistleblowing Research.* Edward Elgar Publishing, Cheltenham, UK, 2014. 1-36. 4. o.

[68] Burai Petra: *Koncepció a közérdekű bejelentések (whistleblowing) törvényi szabályozásához*. Transparency International Magyarország, 2008

Magyarországon alkalmazott, magyar jogszabályi háttérrel is rendelkező jogintézménynek szükséges magyar elnevezést adni, e tanulmány – tipikusan a jelenség általános ismertetése során – mégis inkább az autentikus whistleblowing terminus technicus használta mellett foglal állást, hiszen ha az eredeti kifejezést és annak magyar megfeleltetését mind etimológiai, mind tartalmi vizsgálat tárgyává tesszük, látható, hogy a két fogalom nem fedi teljes mértékben egymást.[69]

A fent definiált whistleblowing genus proximuma a gazdálkodó szervezeten belüli jogsértés jelentése, megfelelő szervek tudomására hozása, azaz e fogalmi elem adja meg jelenség *lényegét*. Fontos azonban a többi ismérvről is szót ejteni, hiszen valódi whistleblowing-ról csak ezek teljesülése esetén beszélhetünk. A whistleblowing határainak meghúzásához három lényegi ismérv mentén történő meghatározás szükséges: vizsgálandó elsősorban a whistleblower *személye*, a whistleblowing *címzettje*, valamint annak *tárgya*, azaz a nyilvánosságra hozott információ tartalma.[70]

Mindenekelőtt fontos rögzíteni, hogy whistleblower-nek csak insider informátor minősül,[71] azaz olyan személy, aki az érintett gazdálkodó szervezetnek valamilyen módon részét képezi (vagy képezte),[72] annak tagja, vagy azzal munkaviszonyban vagy munkavégzésre irányuló egyéb jogviszonyban áll, azaz az információt mint annak belső birtokosa hozza nyilvánosságra.[73] Ilyen módon tehát a whistleblower-nek személyes kvalifikációval kell rendelkeznie.

Az információ közlésének címzettjét tekintve különbséget kell tennünk az ún. belső (intern), valamint a külső (extern) whistleblowing között. Amíg *belső* (vagy zárt)[74] whistleblowing esetén a címzett a whistleblower személyéhez hasonlóan a gazdálkodó szervezet részét képező szerv (vagy személy),[75] addig *külső* (azaz kifelé irányuló) whistleblowing esetén a belső információ kikerül a gazdálkodó szervezet keretei közül,[76] így valódi, szoros értelemben vett nyilvánosságra hozatalról ez utóbbi esetben beszélhetünk.[77] A német szakirodalom a tisztán külső, valamint tisztán belső címzetti körön kívül definiál egy köztes pozíciót is, mégpedig az ún. *ombudsman*[78]

---

[69] Érzékelhető, hogy a fogalom értékeléssemlegességre törekszik – amely törekvésnek eleget is tesz, azaz sem negatív (pl. besúgó, denunciátus), sem kifejezetten pozitív tartalmat nem vetít előre, azonban mégis hiányzik belőle annak a funkciónak az érzékeltetése, amely a whistleblowing elsődleges célja: veszély, illetve sérelem bekövetkezésének megelőzése, illetőleg ha már bekövetkezett, annak hatékony orvoslásához, felderítéséhez, represszálásához vezető út whistleblower általi megnyitása.

[70] Molnár: *A közérdekű bejelentés bűnmegelőzési és bűnfelderítési relevanciájának vizsgálata a gazdálkodó szervezeten belül elkövetett bűncselekmények vonatkozásában* 80. o.

[71] Hefendehl: i.m. 619. o.; Lewis – Brown – Moberly i. m. 5. o.

[72] Rotsch-Wagner: i.m. 1314. o.

[73] *Uo.*

[74] Böckler: i.m. 12. o.

[75] Pl. vezető tisztségviselő, felügyelőbizottság, compliance officer, vagy kifejezetten e jelentések fogadására létrehozott belső szerv. Vö. Rotsch-Wagner: i.m. 1317. o., Böckler: i.m. 17. o.

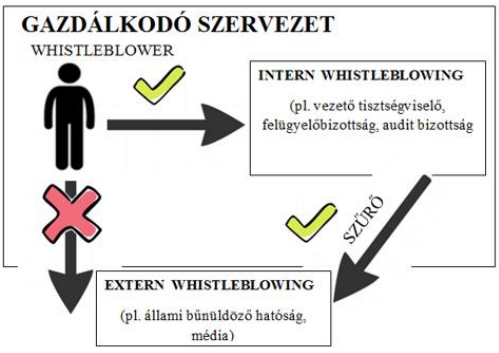
[76] Koch, Arnd: Korruptionsbekämpfung durch Geheimnisverrat? Strafrechtliche Aspekte des Whistleblowing. *Zeitschrift für Internationale Strafrechtsdogmatik* 10/2008, 502. o.

[77] Legtágabb értelemben a nyomozóhatóságot, valamint a médiát is a külső whistleblowing címzettjének tekintjük. Vö. Hefendehl: i.m. 619. o, Böckler: i.m. 6. o.

[78] Az ombudsman megnevezés tehát nem egy állami szervet jelöl, hanem azon személy (pl. egy ügyvéd), aki köztes helyet foglal el a whistleblowing két, általános címzetti köréhez képest. Vö. Simonet, Michael:

személyét, aki alapvetően nem képezi a szervezet részét, azaz formálisan külső személynek tekintendő,[79] azonban kifejezetten a bejelentések fogadásának céljából szerződéses jogviszonyban áll azzal.

5.2. A whistleblowing potenciális relevanciája vállalati titok védelme terén. Főszabály szerint sem hazánkban, sem nemzetközi színtéren nincsen általános kötelezettség a szervezeten belüli whistleblowing-rendszer kiépítésére nézve, az mégis üdvözlendő és – bármily meglepő – elsősorban a szervezet számára előnyös megoldás. Ennek az az oka, hogy a – még büntetőjogilag nem releváns, de e veszélyt potenciálisan magában rejtő – visszaélések belső kezelése képes lehet megóvni a szervezetet jó hírnevének elvesztésétől,[80] a számára tipikusan nemkívánatos külső whistleblowing-tól,[81] emellett pedig jelentős kriminálpreventív hatással is bír. A jogintézmény fontosságát, preventív hatását az uniós jogalkotó is felismerte, a szervezeti visszaéléseket bejelentő személyek fokozott védelmét hivatott garantálni az uniós jog megsértését bejelentő személyek védelméről szóló 2019/1937 irányelv.[82] A Bejelentővédelmi irányelv 4. cikke tartalmazza azokat az esetköröket, amikor a jelentéstételre, valamint a jelentések nyomon követése céljából az irányelv tárgyi hatály alá tartozó szervezetek kötelesek belső csatornát létrehozni, bejelentéssel kapcsolatos belső eljárást kidolgozni. A whistleblowing intézmény kriminálpreventív jellemvonása hordozza magában az üzleti titok védelmére való alkalmasságát. Hogyan képes azonban egy olyan intézmény a vállalati titok védelmére, amely éppen, hogy információk nyilvánosságára hozatalát hivatott szolgálni? Miképpen nyerhet igazolást e paradoxonnak tűnő hipotézis? A kérdés megválaszolásához a fentebb tárgyalt fogalmi elemek közül a whistleblowing címzettjét kell megvizsgálni, azaz a nyilvánosságra hozást belső, valamint külső nyilvánosságra kell kettéválasztanunk. A hipotézist a következő ábra segítségével kívánom igazolni:



(2. ábra)

Die 1 Berlin, Logo

[79] *Uo.* 8. o.

[80] *Uo.* 16. o.

[81] Koch: i.m. 502. o.

[82] Az Európai Parlament és a Tanács (EU) 2019/1937 irányelve (2019. október 23.) az uniós jog megsértését bejelentő személyek védelméről, HL L 305. *(továbbiakban: Bejelentővédelmi irányelv)*

A külső és a belső whistleblowing közötti jellegadó különbség az, hogy eltérő az információ címzettje. Addig, amíg belső whistleblowing esetén a címzett a szervezet részét képező szerv vagy személy (azaz az információ szolgáltatójával megegyezően insider), addig a külső whistleblowing esetén a gazdálkodó szervezeten kívül eső, külső szerv vagy személy.[83] A külső whistleblowing jelentős veszélyeket rejt magában, hiszen – mint ahogyan az az ábrán is látható – a whistleblower a tudomására jutott jogsértést közvetlenül külső szerv, avagy a média tudomására hozza, azaz a szó legszorosabb értelmében nyilvánosságra hozza azt. Éspedig amennyiben a jogsértéssel üzleti titok is nyilvánossága kerül, úgy a folyamat, amely a gazdálkodó szervezet jó hírnevét, valamint gazdasági versenyhelyzetét negatíve érinti, tulajdonképpen irreverzibilis, ugyanis az üzleti titok védett volta *(tulajdonképpen „titok volta")* annak megismerésével, titokjellegének megszűnésével elvész.[84] Ezzel szemben amennyiben a szervezet olyan megfelelő, belső fórumot épít ki, amelynek célja és rendeltetése az, hogy a jogsértést a szervezet tagja, illetve dolgozója jelentse, és ehhez megfelelő motivációt is biztosít számukra, úgy a jól működő internal whistleblowing szervezet működésére gyakorolt pozitív hatása vitathatatlan. Ugyanis azzal, hogy a tényleges vagy potenciális jogsértést a whistleblower a szervezet arra jogosult szerve tudomására hozza, úgy e szerv vagy személy tulajdonképpen mintegy *szűrő* szerepet lát el, azaz egyrészről lehetőség adódik arra, hogy a jogsértés tényállásának felderítésére a szervezeten belül kerüljön sor,[85] másrészt pedig – a szervezeten belüli felderítés alapján feltárt tényállásnak megfelelően – lehetősége van arra, hogy a jogsértést, valamint – potenciálisan – a felderítésének eredményét az üzleti hírnevét, gazdasági versenyhelyzetét sértő vagy veszélyeztető, szenzitív információk, adatok nélkül hozza a külső szervek, illetve a média tudomására.

A belső whistleblowing know-how-t védő hatásával kapcsolatban felállított hipotézist támasztja alá az *Európai Parlament és a Tanács (EU) 2016/943 irányelve (2016. június 8.) a nem nyilvános know-how és üzleti információk (üzleti titkok) jogosulatlan megszerzésével, hasznosításával és felfedésével szembeni védelemről* törekvése. Az irányelvben meghatározott szankciók azzal szemben alkalmazhatók,

---

[83] Molnár: *A közérdekű bejelentés bűnmegelőzési és bűnfelderítési relevanciájának vizsgálata a gazdálkodó szervezeten belül elkövetett bűncselekmények vonatkozásában* 81. o, vö. Ambrus-Farkas: i.m. 2020. o.

[84] Faludi: i.m. 63. o., Fézer Tamás: Személyiségi jogok, in: *A polgári törvénykönyvről szóló 2013. évi V. törvény és a kapcsolódó jogszabályok nagykommentárja. I. kötet*. (szerk: Osztovits András), Budapest, Opten Informatikai Kft. 2014, 297. o, 300. o.

[85] Az internal whistleblowing tulajdonképpen a compliance-management represszív aspektusának részét képezi, egyúttal quasi belső nyomozási eljárás megindítását indukáló cselekménynek is tekintendő, ugyanis azzal, hogy eszköz arra, hogy a jogsértés a szervezeten belül meghatározott személy vagy szerv tudomására jusson, megteremti a lehetőséget a szervezeten belüli kivizsgálásra, ún. internal investigaton eljárás lefolytatására. [Internal investigation témáról lásd részletesen: Molnár Erzsébet: A vállalkozáson belüli előnyomozási eljárás interdiszciplináris kontextusban. *Jogtudományi Közlöny* 2016/9, 458-468. o., vö. Ambrus-Farkas: i.m. 207. o.)

aki az abban meghatározott magatartások valamelyikének realizálásával üzleti titkot sért (4. cikk). Az irányelv 5. cikke tartalmazza azonban azokat az esetköröket, amikor is az üzleti titok megszerzése, felhasználása, illetve felfedése nem minősül jogszerűtlennek, ennek megfelelően az abban meghatározott szankciók – így büntetőjogi szankciók – sem alkalmazhatók. Az irányelv e rendelkezésében jogellenességet kizáró körülménynek tekinti azt az esetet, amikor a munkavállalók az üzleti titkot a szervezet reprezentatív funkcióikat jogszerűen gyakorló képviselőik előtt fedik fel [5. cikk c) pont]. Az irányelv ezen rendelkezései is átültetésre kerültek az Üttv.-be.[86] E rendelkezés magában hordozza azt a törekvést is, hogy az munkavállaló, akinek valamilyen – üzleti titokkal kapcsolatba hozható – szervezeten belüli jogsértés tudomására jut, úgy azzal elsősorban szervezeten belüli szervhez vagy személyhez forduljon, ezáltal az üzleti titok nyilvánosságra hozása miatt rendelkezésre álló szankciók vele szemben – jogellenesség hiányában – nem lesznek alkalmazhatók. Ugyanis az üzleti titok minél kiterjedtebb védelme a minőségi kutatás ösztönzésének, az innovatív gondolkodás kibontakozásának irányába hat.

6. Összegzés

A vállalati titok szűk körben, az „érintettekkel" történő megosztása elengedhetetlen ahhoz, hogy az innováció, titokban tartott *találmány* alkalmas legyen azt a célt szolgálni, amiért tipikusan készült: a szervezet versenyképességének megőrzését, javítását, a tudomány fejlődését. Éppen ezért a titoknak a munkavállalókkal való megosztása – mint láthattuk – kockázati tényező, ámde olyan rizikófaktor, amelyet vállalni szükséges az ismeret optimális kihasználása érdekében. Ahogyan a gazdálkodó szervezet, vállalkozás mint zárt entitás, mint közös cél irányába tartó személyek összessége, képes arra, hogy innovatív megoldásokat fejlesszen ki, majd azokat gazdaságilag hasznosítható módon alkalmazza is, éppen úgy e munkavállalók jelentik potenciálisan az egyik legnagyobb veszélyt is a szervezet gazdasági létére. Ugyanis a vállalati titoknak a rendelkezésükre bocsátása egy szükségképpeni bizalmi kapcsolatot teremt, és e tudás, ismeret mindenkor alkalmas eszköz azon munkavállaló kezében, akit esetlegesen sérelem ér a szervezet részéről, vagy pusztán az ismeret áruba bocsátásával anyagi haszonra kíván szert tenni. Az üzleti titok, valamint know-how rendkívül szenzibilis jogi kategóriák, ugyanis a titokjelleg megszűnése[87] a védelem visszafordíthatatlan megszűnését is jelenti egyben (feltéve, hogy egyéb oltalomban nem részesíthető ismeretről van szó). Az üzleti titok, tipikusan a know-how sérülékenysége miatt pedig fokozott védelmet igényel, a védelmi rendszer megteremtése pedig szervezeti érdek. A titok potenciális elveszítése kockázatának felmérése, és adekvát védelmi rendszer kiépítése tipikusan szervezeti feladat, a szervezet CMS-ének szerves részét képező probléma. A szervezeten belüli védelmi rendszeren túl a jogi védelem eszközei számos jogág keretein belül adottak. A titoksértővel szembeni represszív – legyen az akár magánjogi, akár büntetőjogi – szankció alkalmazásával a megsértett jogrend

[86] Sántha: i.m. 48-49. o.
[87] Frank: i.m. 41. o.

látszólag helyreáll ugyan, a már említett irreverzibilitás miatt a szervezet azonban de facto nem orvosolható sérelmet szenved. Mindebből következik, hogy elsődleges cél a jogellenes cselekmény, bűncselekmény elkövetésének megelőzése, amely, mint láthattuk, leginkább a szervezeten belüli intézkedések foganatosításával garantálható. A titokvédelem a titok jogosultjának elsődleges érdeke. A gazdálkodó szervezet javát szolgáló titok jogosultja tipikusan a szervezet vezetője, így őt terheli a szervezeti érdeket szolgáló, megfelelő védelmi rendszer kiépítésének kötelezettsége. E rendszer visszaélés-felderítő aspektusa az ún. internal whistleblowing rendszer, amely – mint láthattuk – ha szűk körben is, de alkalmas lehet arra, hogy megvédje a szervezetet az üzleti titok nyilvánosságra hozásától.