

PLATFORMELE DE CROWDFUNDING LA GRANIȚA DINTRE SECURITATE ȘI FRAUDĂ

CROWDFUNDING PLATFORMS AT THE BORDER BETWEEN SECURITY AND FRAUD

DESPINA-MARTHA ILUCĂ¹
ALIN CIPRIAN SIMION²

Rezumat: În mecanismul de *crowdfunding* ca nouă formă de finanțare participativă, platforma online are o importanță deosebită, fiind mai mult decât un simplu intermediar. Rolul platformei este incontestabil, încât apreciem că existența unei platforme reprezintă o condiție *sine qua non* pentru calificarea unei operațiuni ca fiind de finanțare participativă. Astfel, considerăm esențială cercetarea aspectelor privind funcționarea platformei de *crowdfunding*, pentru a explica mecanismul acesteia și pentru a deduce o serie de reguli de conduită pe care le vom trata în mod distinct. În paralel cu planul juridic și economic, vom analiza o parte dintre vulnerabilitățile sistemului informatic asociat tranzacțiilor online în mecanismul de *crowdfunding*, încercând să determinăm dacă protecția și securitatea promisă utilizatorilor platformei este una reală.

Cuvinte cheie: platformă, finanțare participativă, crowdfunding, vulnerabilitate sistem informatic, tranzacție online

Abstract: In the mechanism of crowdfunding as a new form of collaborative financing, the online platform is particularly important, being more than just a simple intermediary. The role of the platform is indisputable as to the point in which it is a *sine qua non* condition for qualifying an operation as crowdfunding. Therefore, we find it essential to research the aspects regarding the functioning of the crowdfunding platform, in order to explain its mechanism and to deduce a series of rules of conduct. Apart from the legal and economical standpoint, we will analyze some vulnerabilities of the system associated with online crowdfunding transactions,

¹ Doctorand, Universitatea „Alexandru Ioan Cuza” din Iași, Facultatea de Drept, email: despina.iluca@gmail.com.

² Doctorand, Universitatea „Alexandru Ioan Cuza” din Iași, Facultatea de Informatică; Security Researcher, Bitdefender, email: asimion@bitdefender.com.

in an attempt to determine whether the promised user protection and security is indeed a real one.

Keywords: platform, collaborative financing, crowdfunding, system vulnerability, online transaction

1. Aspecte introductive privind operațiunile de *crowdfunding*. Argument pentru importanța platformelor online de finanțare participativă

Crowdfunding-ul reprezintă o formă de finanțare prin care un număr mai mare de persoane contribuie cu sume relativ mici prin intermediul unei platforme online, pentru susținerea unei inițiative, de regulă un *start-up*, sau pentru dezvoltare întreprinderilor mici și mijlocii³. Această activitate se desfășoară fie în schimbul unui câștig sau, cel puțin, a recuperării investiției, fie fără a urmări vreun fel de recompensă⁴.

Astfel, într-o clasificare sintetică, în funcție de beneficiile obținute de finanțator în urma contribuției sale, *crowdfunding*-ul se împarte în două categorii: (1) *investment-based model*: este forma prin care se urmărește obținerea de profit (în sens larg), fie sub forma unui procent din câștigurile viitoare, respectiv dividendul primit ca urmare a dobândirii calității de acționar și a realizării de profit de către companie (*equity crowdfunding*), fie prin rambursarea împrumutului cu dobândă (*crowdlending/debt crowdfunding*) și (2) *non-investment-based model*, în care finanțatorii fie nu urmăresc obținerea vreunei recompense în bani (*donation-based crowdfunding*), fie au doar așteptarea unei recompense în bunuri simbolice, de valoare mică prin comparație cu suma oferită (*reward-based crowdfunding*)⁵.

Clasificând operațiunile de *crowdfunding* după un al doilea criteriu, respectiv în funcție de atingerea plafonului minim necesar pentru finanțare, se disting două categorii: (1) *Keep-it-All* sau „Păstrează tot ce câștigi” și (2) *All-or-Nothing* sau „Totul sau nimic”. Aplicarea sistemului *Keep-it-All* în *crowdfunding* implică păstrarea de către beneficiarul finanțării

³ C.T. Ungureanu, *Dreptul comerțului internațional*, Editura Hamangiu, București, 2018, p. 304.

⁴ J. Armour, L. Enriques, *The Promise and Perils of Crowdfunding: Between Corporate Finance and Consumer Contracts*, Oxford Legal Studies Research Paper No. 58/2017, [Online] la https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3035247##, accesat 12.11.2018.

⁵ R. Perry, *Crowdfunding Civil Justice*, Boston College Law Review, Vol. 59, pp. 1359-1360, [Online] la https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3041129, accesat 12.11.2018.

a tuturor sumelor primite, indiferent dacă s-a atins sau nu ținta prestabilită (*preset capital goal*). Pe de cealaltă parte, sistemul *All-or-Nothing* presupune restituirea contribuțiilor în cazul în care plafonul minim de finanțare nu este atins. Importanța acestei clasificări rezidă și în riscul pe care și-l asumă finanțatorii, întrucât în sistemul *All-or-Nothing* aceștia sunt protejați de riscul cheltuirii aparent inutile unor sume de bani pentru inițiative sub-finanțate⁶.

Finanțările participative sunt o practică veche, însă elementul de noutate constă tocmai în utilizarea unei platforme online pentru strângerea fondurilor⁷. Cel puțin în privința finanțării companiilor, în mod tradițional, micile întreprinderi obțineau finanțare alternativă creditelor bancare de la ceea ce unii autori⁸ numesc „cei trei F” (din engleză, *the three 'f's: family, friends and fools*): familie, prieteni și nebuni, însă aceste surse se pot dovedi adesea insuficiente. În perioada recentă, *business angels* și *venture capitalists* – sursele clasice pentru obținerea unui capital de risc după epuizarea celor „trei F” – au început treptat să realizeze investiții în companii mai dezvoltate. Spre exemplu, un număr crescut de *business angels* sunt interesați doar de afaceri care solicită finanțare de peste 100.000 dolari⁹, în timp ce mecanismul de *venture capital* este mai complex, implicând o companie specializată în acest sens, care oferă finanțare de ordinul milioanei de dolari (sume care adesea provin din alte surse, de tipul fondurilor de pensii) și numesc un membru în organele de conducere ale *start-up*-ului finanțat. Prin comparație, *equity crowdfunding* asigură finanțarea cu sume cuprinse, în medie, între 50.000 și 100.000 dolari¹⁰.

În cadrul acestor forme de finanțare în plină dezvoltare, considerăm că o importanță deosebită o au platformele de *crowdfunding*, care, de multe ori, îndeplinesc mai mult decât un simplu rol de intermediar.

⁶ M. Gomez, *Crowdfunded Justice: On the Potential Benefits and Challenges of Crowdfunding as a Litigation Financing Tool*, 49 U.S.F. L.Rev. 307 (2015), p. 312, [Online] la http://collections.law.fiu.edu/faculty_publications/201/, accesat 12.11.2018.

⁷ C.T. Ungureanu, *op.cit.*, p. 304.

⁸ L. Pelizzon, M. Riedel, P. Tasca, *Classification of Crowdfunding in the Financial System*, în volumul *Banking Beyond Banks and Money*, Springer International Publishing Switzerland, 2016, p. 11.

⁹ K.E. Wilson, M. Testoni, *Improving the Role of Equity Crowdfunding in Europe's Capital Markets*, Social Science Research Network Working Paper Series (2014), apud L. Pelizzon, M. Riedel, P. Tasca, *op.cit.*

¹⁰ *Ibidem*.

Există în doctrină și opinia¹¹ conform căreia trăsătura definitorie a *crowdfunding*-ului nu este neapărat modul prin care se colectează sumele (printr-o platformă online), ci faptul că acestea provin de la un număr considerabil de persoane (de la *crowd*), dispersați din punct de vedere geografic¹² și a căror contribuție poate fi condiționată de expectanța unui câștig care variază de la beneficii intangibile și până la recompense materiale. Cu toate acestea, apreciem că în lipsa unui instrument online, *crowd*-ul dispersat geografic nu ar putea să contribuie, astfel că existența unei platforme se constituie într-o condiție *sine qua non* pentru calificarea unei operațiuni ca fiind de *crowdfunding*.

În acest context, o noțiune conexasă apare ca relevantă în discuție, cea de „economie colaborativă”. Conceptul desemnează emergența unei noi forme de consum, favorizată de creșterea numărului de platforme online pentru interconectarea persoanelor și de dezvoltarea erei informatizate¹³. În prezent, inițiativele originale și platformele colaborative înfloresc în toate sectoarele de activitate: de la folosirea în comun a unui bun sau a unui serviciu și chiar până la finanțarea participativă a litigiilor (fenomen cunoscut sub denumirea de *crowd litigation funding*).

Astfel, platformele de *crowdfunding* asigură o serie de sarcini administrative și chiar fiduciare prin procedurile pe care le elaborează și le implementează în activitatea de colectare, gestionare, cheltuire și eventual rambursare a sumelor de bani¹⁴. Mai mult decât atât, acestea au început să dezvolte procedee de selecție transparentă a inițiativelor pe care le acceptă pentru finanțare prin intermediul platformei, pentru a diminua riscurile asociate cu tranzacțiile online și pentru a construi un mediu de confort pentru finanțatori, prin acordarea unor minime garanții de protecție a drepturilor lor. Pentru acoperirea costurilor operaționale și pentru a genera un profit din această activitate, platformele rețin un procent (în medie 3-10%) din sumele obținute de beneficiar¹⁵.

¹¹ M. Gomez, *op.cit.*, p. 313.

¹² În ceea ce privește dispersarea geografică în *crowdfunding*, a se vedea A.K. Agrawal, C. Catalini, A. Goldfarb, *The Geography of Crowdfunding*, Nat'l Bureau of Econ. Research, Working Paper No. 16820, Feb. 2011, [Online] la <http://www.nber.org/papers/w16820.pdf>, accesat 12.11.2018, *apud* M. Gomez, *op.cit.*

¹³ M. Moulai (ed.), *Tout se partage, tout s'échange. Le guide pratique*, Particulier et Finances Éditions, Paris, 2018, p. 15.

¹⁴ M. Gomez, *op.cit.*, p. 311.

¹⁵ R. Perry, *op.cit.*, p. 10.

2. Limite și provocări în funcționarea platformelor de *crowdfunding*

Caracterul predominant internațional al operațiunilor de *crowdfunding*, precum și operarea platformelor transfrontalier, generează o serie de întrebări de natură juridică și probleme de proveniență tehnică, pe care le vom trata în secțiunile ce urmează în prezentul studiu, însă fără pretenția unui demers exhaustiv. În final, intersectând planul normativ cu cel al informaticii, vom încerca să determinăm provocările comune celor două.

2.1. *Mecanism contractual și lege aplicabilă. Oportunitatea unei reglementări speciale în materie*

Expresia juridică de transpunere a operațiunilor de *crowdfunding* în practică este reprezentată de contractul de *crowdfunding*, pornind de la mecanismul contractual general al acestor operațiuni, care se configurează într-o schemă triunghiulară a raportului contractual dintre platformă și titularul de proiect, raportul contractual dintre platformă și finanțator, precum și raporturile care se stabilesc între titularul de proiect și finanțator¹⁶.

În privința contractelor, prima problemă tratată este aceea a încheierii electronice a acestora, prin prisma teoriei încheierii contractelor la distanță, dar și sub un alt aspect foarte important, al posibilității de negociere a unui astfel de contract.

Astfel, raportându-ne la condițiile de validitate ale actului juridic civil, în ceea ce privește consimțământul, subiectul suscită multiple discuții de natură juridică referitor la contractul care se încheie între utilizator și platformă. În primul rând, este necesar să precizăm că aceste contracte electronice sunt contracte de adeziune¹⁷, luând forma unor *Terms and Conditions* sau *Terms of Use*.

În al doilea rând, având în vedere clasificarea contractelor electronice după modul de încheiere în contracte *click-wrap/click-through*, contracte *browse-wrap* și contracte care poartă o semnătură electronică extinsă calificată¹⁸, constatăm că cel puțin în privința contractelor încheiate

¹⁶ C.T. Ungureanu, *op.cit.*, p. 308.

¹⁷ În acest sens, a se vedea, C.T. Ungureanu, *Contractul electronic*, în Revista „Dreptul” nr. 9/2015, pp. 158-185, C.T. Ungureanu, *The Effectiveness of Certain Contractual Clauses in a Transnational Electronic Contract of Adhesion*, în Supliment la Revista „Universul Juridic”, 2016, pp. 247-251.

¹⁸ În acest sens, a se vedea, C.T. Ungureanu, *Implicațiile Internetului în viața juridică*, în Analele Științifice ale Universității „Al. I. Cuza” Iași, Tomul LXIII, Științe juridice, nr.

între platformă și utilizator (fie că este finanțator, fie că este beneficiarul finanțării), aceste contracte sunt *browse-wrap*¹⁹. Mai mult decât atât, exemplele studiate conțin clauze prin care platforma poate modifica unilateral termenii acordului, fără a fi necesară notificarea prealabilă a utilizatorilor și fără a putea fi obligată la daune, precum și multiple alte clauze exoneratoare de răspundere a platformei.

În aceste condiții, ne întrebăm dacă ne aflăm în prezența unui consimțământ „forțat”, de tipul *take it or leave it*, dat fiind faptul că negocierea clauzelor contractuale este cvasi-imposibilă, iar majoritatea covârșitoare a utilizatorilor nu citește termenii și condițiile și nu au reprezentarea faptului că simpla folosire a platformei implică încheierea unui contract²⁰.

În egală măsură, ceea ce interesează sub aspect juridic este problema legii aplicabile contractului, cu precădere din considerentul caracterului internațional pe care îl poate avea o operațiune de *crowdfunding*, platforma fiind înregistrată într-un stat, iar utilizatorii putând proveni din alte state. De cele mai multe ori, determinarea legii aplicabile se realizează în conținutul contractului, adică în clauzele *Terms and Conditions/Terms of Use*, și este stabilită în majoritatea cazurilor și în mod previzibil ca fiind legea statului în care este înregistrată platforma²¹. De altfel, și modalitatea de

2/2017, pp. 1-20, [Online] la http://pub.law.uaic.ro/files/articole/2017/volii/1.ungureanu_implicatiile_internetului.pdf, accesat 12.11.2018.

¹⁹ Kickstarter: “By using this website (the “Site”) and services (together with the Site, the “Services”) offered by Kickstarter, PBC (together with Drip U.S., LLC, The Creative Independent, LLC, and its and their parents, subsidiaries, affiliates, agents, representatives, consultants, employees, officers, and directors — collectively, “Kickstarter,” “we,” or “us”), you’re agreeing to these legally binding rules (the “Terms”). You’re also agreeing to our Privacy Policy and Cookie Policy, and agreeing to follow any other rules on the Site, like our Community Guidelines and rules for starting projects.”, [Online] la <https://www.kickstarter.com/terms-of-use?ref=global-footer>, accesat 12.11.2018.

Crowdcube: “By using this Site, you indicate that you accept these terms of use and that you agree to abide by them. If you do not agree to these terms of use, please refrain from using this Site.”, [Online] la <https://www.crowdcube.com/pg/terms-16>, accesat 12.11.2018.

Wiseed: “Tout accès ou utilisation du site www.wiseed.com (ci-après le « Site ») vaut acceptation sans réserve des présentes Conditions Générales d'Utilisation.”, [Online] la <https://www.wiseed.com/fr/conditions>, accesat 12.11.2018.

²⁰ În acest sens, a se vedea și C.T. Ungureanu, *Implicațiile Internetului (...)*, p. 4.

²¹ Kickstarter: “In the unfortunate situation where legal action does arise, these Terms (and all other rules, policies, or guidelines incorporated by reference) will be governed by and construed in accordance with the laws of the State of New York and the United States, without giving effect to any principles of conflicts of law, and without application of the

soluționare a litigiilor, precum și instanța competentă sunt indicate în condițiile de utilizare prin clauze – exclusive sau nu, după caz – atributive de competență.

Sub aspectul reglementării operațiunilor de *crowdfunding*, în special prin intermediul unor instrumente care să răspundă dificultăților rezultate din caracterul internațional al acestor tranzacții, observăm o recentă schimbare de paradigmă a Comisiei Uniunii Europene referitoare necesitatea reglementării *crowdfunding*-ului, cu precădere în privința platformelor. Printr-o comunicare publicată de Comisie în 2014 se aprecia că nu există argumente care să justifice intervenția de politică la nivelul UE în contextul respectiv. Cu toate acestea, monitorizarea constantă a domeniului și publicarea de către Comisie a Planului de acțiune pentru tehnologie financiară (FinTech) în martie 2018, care exprimă ambiția de a face din Europa un hub FinTech mondial, în care firmele și investitorii din UE să beneficieze cât mai mult posibil de avantajele pieței unice în acest sector cu evoluție rapidă, a condus la reaprecierea asupra subiectului și la schimbarea de optică a Comisiei, concretizată prin Propunerea de regulament al Parlamentului European și al Consiliului privind furnizorii europeni de servicii de finanțare participativă (ECSP) pentru întreprinderi, Bruxelles, 8.3.2018, COM(2018) 113 final²². În expunerea de motive la propunerea de regulament este evidențiată necesitatea de extindere a disponibilității finanțării prin *crowdfunding* „la o scară mai largă, în beneficiul solicitanților de fonduri și al investitorilor din toate statele membre”, având în vedere „tendința continuă de concentrare a sectorului european al finanțării participative în doar câteva state membre”, precum și provocările cu care se confruntă platformele de finanțare participativă când doresc să își extindă

Uniform Computer Information Transaction Act or the United Nations Convention of Controls for International Sale of Goods.”, [Online] la <https://www.kickstarter.com/terms-of-use?ref=global-footer>, accesat 12.11.2018.

Crowdcube: “*The English courts will have non-exclusive jurisdiction over any claim arising from, or related to, a visit to our site although we retain the right to bring proceedings against you for breach of these conditions in your country of residence or any other relevant country. These terms of use are governed by English law.*”, [Online] la <https://www.crowdcube.com/pg/terms-16>, accesat 12.11.2018.

Companisto: “*German law applies exclusively, excluding the UN Sales Convention (CISG). Venue for the settlement of disputes arising from and in relation to this contract shall be Berlin insofar as is permitted by law.*”, [Online] la <https://www.companisto.com/en/page/business-terms>, accesat 12.11.2018.

²² [Online] la <https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52018PC0113&from=EN>, accesat 12.11.2018.

operațiunile pe teritoriul Uniunii. În aceste condiții, soluția unui regulament – cu aplicarea directă a acestuia – este privită de Comisie ca optimă pentru reglementarea unei proceduri de acces de tip „pașaport” pentru platformele care vor dori să furnizeze servicii pe întreg teritoriul Uniunii, cu precizarea că domeniul de aplicare al regulamentului este intenționat a fi limitat la modelele bazate pe investiții și pe creditare, în timp ce finanțarea participativă pe bază de donații și de recompense este exclusă din sfera de aplicare a regulamentului.

Chiar și în lipsa unei reglementări la nivelul UE, statele membre manifestă interes pentru legiferarea fenomenului, dar mai ales a activității platformelor, prin impunerea unor reguli de conduită. Cu titlu exemplificativ, proiectul de lege din România privind dezvoltarea finanțărilor participative (înregistrat la Camera Deputaților cu nr. 801/09.11.2015) statuează cu titlu de principiu general că *„Platformele de finanțare participativă trebuie să funcționeze în conformitate cu principiile de neutralitate, transparență și diligență și în conformitate cu protejarea intereselor clienților lor”*, protecție care se poate realiza prin impunerea în sarcina platformei a unei obligații de informare cu privire la modul de funcționare, riscuri, nivelul comisioanelor, precum și prin gestiunea conflictului de interese și prin interdicția ca platforma să participe la proiecte. State precum Franța au creat chiar și noi forme dedicate statutului juridic al platformelor, respectiv: consilier în investiții participative (*conseiller en investissements participatifs*) și intermediar în finanțări participative (*intermédiaire en financement participatif*), ambele forme fiind supuse unor proceduri de înregistrare și având autorități de reglementare distincte²³.

2.2. Protecția împotriva atacurilor cibernetice. Securitate și algoritmi de criptare

Platformele de *crowdfunding*, la fel ca orice platformă online prin intermediul căreia se derulează tranzacții financiare, pot fi ținta atacurilor cibernetice. În mod evident, prima întrebare care se ridică este: cine sunt atacatorii? Impresia generală a publicului larg este că atunci când are loc un atac, în spatele lui este un singur individ, aspect care se adevărește în cazul

²³ K. Boyer, A. Chevalier, J.-Y. Léger, A. Sannajust, *Le crowdfunding*, Éditions La Découverte, Paris, 2016, pp. 41-42.

unor atacuri accidentale sau minore. Însă atunci când în discuție sunt atacuri cu impact financiar – sau chiar politic – de amploare, realitatea ne arată că acestea sunt puse în scenă de grupări infracționale organizate, care beneficiază de multiple resurse și dețin cunoștințe tehnice avansate.

Un exemplu de astfel de atac este APT28. *Advanced persistent threat 28* sau „amenințări avansate persistente” sunt denumiri primite de atacuri cu impact major sau bănuite a fi finanțate politic. APT28 sau Sofacy a fost un atac despre care se crede că avea ca țintă instituții statale din țări precum Ucraina, România, Bulgaria, Spania, Rusia, Statele Unite ale Americii sau Canada. Atacul a fost inițiat prin scanarea a peste 8 milioane de IP-uri pentru identificarea de vulnerabilități tehnice. În urma analizei atacului, s-a constatat copierea fișierelor ce conțineau arhive de e-mail²⁴.

În vederea diminuării riscurilor unor atacuri informatice, utilizatorii își pot lua o serie de măsuri de precauție prin realizarea unei examinări preliminare a platformei pentru identificarea așa-numitelor *red flags* (steaguri roșii). Unul dintre primele semne pozitive ale garanțiilor de securitate ale unei platforme este reprezentat de pictograma sub forma de lacăt de culoare verde din dreptul adresei paginii de Internet respective (URL-ul), lacăt care indică faptul că platforma folosește certificate de securitate²⁵. Aceste certificate sunt emise de o autoritate de certificare (*certificate authority*) și informează *browser*-ul utilizatorului cu privire la protocolul de comunicare ce va fi folosit în continuare, mai exact despre metoda de criptare și alți parametri folosiți de aceasta. Autoritățile de certificate emitente ale certificatelor în discuție sunt instituții mondiale, bazate pe principii de transparență, astfel că *browser*-ele au încă de la instalare multe dintre certificatele cel mai des folosite. Astfel, în momentul înțierii conexiunii dintre utilizator și platformă, singura informație schimbată necriptată este certificatul de securitate ce va fi folosit în continuare pentru comunicare.

²⁴ R. Benchea, C. Vatamanu, A. Maximiciuc, V. Luncașu, *APT28 Under the Scope: A Journey into Exfiltrating Intelligence and Government Information*, Bitdefender White Paper, [Online] la https://download.bitdefender.com/resources/media/materials/white-papers/en/Bitdefender_In-depth_analysis_of_APT28%E2%80%93The_Political_Cyber-Espionage.pdf, accesat 12.11.2018.

²⁵ Pentru detalieri în privința certificatelor de securitate, a se vedea *Beginner's Guide to SSL Certificates: Making the Best Choice When Considering Your Online Security Options*, Symantec White Paper, [Online] la https://www.websecurity.symantec.com/content/dam/websecurity/digitalassets/desktop/pdfs/whitepaper/beginners-guide-to-SSL-certificates_WP.pdf, accesat 12.11.2018.

Lipsa pictogramei cu lacătul verde ar trebui să constituie un puternic element descurajant pentru utilizatori în continuarea interacțiunii cu acea platformă. Criptarea comunicării nu înseamnă neapărat o măsură în plus luată pentru siguranță, ci în sine asigurarea că „dialogul” cu aplicația web este confidențială. În lipsa criptării, pot fi interceptate datele trimise către platformă (date cu caracter personal, parole, conturi bancare etc.) sau cele primite de la platformă (parola generată în urma pierderii, coduri pin generate, *token*-uri de logare etc.), folosind tehnici apreciate de profesioniștii în domeniul informatic ca fiind relativ lipsite de complexitate. În acest context, continuarea comunicării cu platforma reprezintă acceptarea de către utilizator a faptului că datele interschimbate pot deveni publice.

Criptarea a cunoscut mai multe îmbunătățiri de-a lungul timpului, luând forma mai multor algoritmi, însă esențialmente, aceasta poate fi împărțită în două mari categorii: (1) criptarea simetrică și (2) criptarea asimetrică. Criptarea simetrică se bazează pe un sistem de două chei, în care mesajul criptat cu prima cheie poate fi decriptat cu cea de-a doua. A doua cheie poate fi obținută matematic din prima, așadar oricine deține una dintre chei o poate afla pe cea de-a doua. O altă trăsătură a criptării simetrice este aceea că lungimea cheilor folosite la criptare este mică sau medie (32-448 biți). Printre exemplele de algoritmi de criptare simetrică se numără DES, 3DES, AES.

Pe de cealaltă parte, criptarea asimetrică este o metoda care implică generarea a patru chei, câte două de către fiecare parte din „dialog”, fiecare având o cheie publică și una privată. Algoritmul este conceput matematic într-o manieră în care cheile nu pot fi generate una din alta. Astfel, niciunul dintre cei doi participanți la comunicare nu poate cripta și decripta mesajul folosind doar cheile sale. În mod diferit față de criptarea simetrică, în criptarea asimetrică lungimea cheilor folosite este mare (1024, 2048, 4096 biți). Cel mai relevant exemplu de algoritm de criptare asimetrică este RSA²⁶, care a fost, de altfel, și primul astfel de algoritm, rămânând cel mai folosit până în prezent.

Cu toate acestea, chiar și folosind certificate de securitate care asigură comunicarea criptată între utilizator și platformă, nu există certitudinea că datele utilizatorului nu vor fi furate. O parte importantă din

²⁶ R.L. Rivest, A. Shamir, L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Massachusetts Institute of Technology, Cambridge, [Online] la <http://people.csail.mit.edu/rivest/Rsapaper.pdf>, accesat 12.11.2018.

comunicarea cu aplicația web este modul în care aceasta stochează datele preluate de la utilizatori, și anume, dacă informațiile sunt păstrate în baza de date în formă criptată sau nu ori într-o altă formă neinteligibilă pentru un necunoscut. Din păcate, nu există autorități în domeniu care să realizeze activitatea de audit sau care să aibă competența de a verifica platformele pentru a determina dacă acestea asigură integritatea datelor preluate și, eventual, să le poată impune un standard minim de securitate.

Unul dintre atacurile care a beneficiat de multă atenție din partea publicului a fost cazul Yahoo. În 2014, baza de date a gigantului Yahoo a fost spartă, fiind colectate date despre peste 500 de milioane de conturi, verificările ulterioare indicând însă că ar exista posibilitatea ca toate cele 3 miliarde conturi ale utilizatorilor Yahoo să fi fost afectate²⁷. Din informațiile oferite către presă, se pare că această companie nu stoca parolele în format lizibil, însă a folosit un algoritm de criptare fără chei, care putea fi inversat. Yahoo și-a anunțat utilizatorii să își schimbe parolele, deoarece au fost pierdut date legate de e-mail, numere de telefon, dar și întrebări de siguranță criptate și necriptate²⁸.

În cazul Yahoo, atacul a provenit din exterior, însă ne întrebăm în egală măsură ce se întâmplă atunci când atacul vine „din interior”. Companiile mai mici care nu au resurse financiare pentru a deține propriile servere, apelează la furnizori de servicii de *hosting* pentru a găzdui platforma. Aceștia din urmă, din considerente de eficiență și optimizare, partajează aceeași unitate virtuală între mai mulți utilizatori, în cazul de față, între clienți care contractează servicii de *hosting*. Din punct de vedere fizic, unitatea virtuală este constituită din mai multe unități *hardware*, astfel că un client nu poate cunoaște cu cine împarte *hardware*-ul. În cadrul unui server, „chiriașii” sunt despărțiți doar logic, virtual, astfel că în cazul descoperirii unei vulnerabilități în această metodă de separație (de obicei, *Firewall*), datele stocate de platformă ar putea fi accesibile și unei terțe părți care se află pe același server. Așadar, se pune problema dacă aplicația web cu care se împarte fizic găzduirea este de bună credință și dacă își ia toate măsurile

²⁷ B. Nelson, *All 3 Billion Yahoo Accounts Have Been Hacked. Here's How You Can Protect Yourself*, Reader's Digest, [Online] la <https://www.rd.com/culture/yahoo-accounts-hacked/>, accesat 12.11.2018.

²⁸ A. Hooper, *Yahoo Downplays Its Billion-Password Security Breach In Emails To Users*, Huffington Post, [Online] la https://www.huffingtonpost.com/entry/yahoo-lost-your-password_us_5852cd15e4b054eeaea218ea, accesat 12.11.2018.

pentru a fi sigură. Chiar și dacă respectiva aplicație nu este una malițioasă în sine, fiind o simplă aplicație de tip broșură sau una de prezentare, care însă nu a investit în securitate, aceasta poate fi o cale de acces către platforma de *crowdfunding* în discuție.

2.3. Linia de convergență între planul juridic și planul informatic

În fața provocărilor juridice și, mai ales, a vulnerabilităților tehnice expuse în cele de mai sus, s-ar părea că dezideratele protecției datelor – nefiind vorba doar de cele cu caracter personal – se află într-o reală primejdie. Ne întrebăm, așadar, dacă mai putem vorbi de o reală protecție a datelor în contextul partajării informațiilor cu alte companii dintr-un grup ori în cazul transmiterii informațiilor către alți terți, fără asigurarea unor garanții adecvate protecției acestora.

Un studiu de caz care ilustrează riscurile amintite anterior este cel al gigantului Facebook, care s-a regăsit și în trecut în mijlocul polemicii privind protecția datelor²⁹ și care joacă rolul unei platforme de *crowdfunding* pentru campaniile sale de *fundraising*. Pentru realizarea acestei activități, Facebook folosește o companie distinctă, Facebook Payments Inc., care recunoaște că în anumite circumstanțe ar putea partaja informațiile cu societatea-mamă, Facebook Inc.³⁰ La rândul său, Facebook Inc. admite posibilitatea transmiterii datelor către alte companii din grup³¹, printre care Onavo, Oculus, WhatsApp și Masquerade.

²⁹ În acest sens, a se vedea cauza Maximilian Schrems împotriva Data Protection Commissioner (C-362/14), [Online] la <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362>, accesat 12.11.2018, în comentariu C.T. Ungureanu, *Protecția datelor cu caracter personal în contractele internaționale*, în *Analele Științifice ale Universității „Al. I. Cuza” Iași*, Tomul LXIII, Științe juridice, nr. 2/2017, pp. 148-149, [Online] la http://pub.law.uaic.ro/files/articole/2017/volii/10.ungureanu_protectia_datelor.pdf, accesat 12.11.2018.

³⁰ Facebook Payments Inc.: “We may share your Personal Information with our parent company Facebook, Inc. This will happen for specific reasons: to process your payment; for maintenance of your payment account; or to detect, prevent, or otherwise address fraud, security, or technical issues.”, [Online] la <https://www.facebook.com/payments/terms/privacy>, accesat 12.11.2018.

³¹ Facebook Inc.: “We may share information about you within our family of companies to facilitate, support and integrate their activities and improve our services (...): Facebook Payments Inc., Onavo, Oculus and Oculus Ireland Limited, WhatsApp Inc. and WhatsApp Ireland Limited, Masquerade, CrowdTangle.”, [Online] la https://www.facebook.com/help/111814505650678?ref=payments_inc_terms, accesat 12.11.2018.

Din păcate, nici alte platforme de *crowdfunding* nu par să ofere decât o protecție iluzorie și strict declarativă a drepturilor utilizatorilor în ceea ce privește protecția informațiilor în cazul transferului de date, în special către furnizorii de servicii conexe de tipul reclame sau chiar către procesatorii externi de plăți, folosind în abundență în *Privacy Policy* modul condițional-optativ prin clauze care preponderent se raliază exprimării „Platforma ar putea să partajeze datele dumneavoastră cu...”³².

Una dintre cele mai cunoscute și folosite platforme de *crowdfunding*, Kickstarter, precizează că atunci când partajează informații cu terții care oferă servicii conexe, le solicită acestora din urmă să folosească datele doar în scopul în care au fost furnizate și să le protejeze cel puțin la aceleași standarde cu cele ale Kickstarter³³. Deși aparent manifestă un grad mai crescut de preocupare pentru securitatea informațiilor și comportă unul dintre primele semne pozitive pentru utilizarea platformei, respectiv existența lacătului de culoare verde în dreptul URL-ului, Kickstarter este un exemplu în care măsurile de precauție luate nu au fost suficiente și o dovadă a faptului că nu există sisteme infailibile, platforma fiind ținta unui atac informatic în anul 2014, în urma căruia atacatorii au obținut nume de utilizatori, adrese de email, numere de telefon și parole. În ciuda faptului că parolele au fost obținute în format criptat, reprezentanții platformei au avertizat utilizatorii că este posibil ca parolele slabe sau evidente să fie descoperite de hackeri, astfel că au încurajat toți clienții să își schimbe parola folosită pentru autentificare³⁴, însă ceea ce constituie o și mai mare sursă de

³² Afirmația are în vedere *Privacy Policy* pentru platformele Kickstarter <https://www.kickstarter.com/privacy?ref=global-footer>, Crowdcube <https://www.crowdcube.com/pg/privacy-and-cookie-policy-17>, FundedByMe <https://www.fundebyme.com/en/privacy-policy/>, Indiegogo <https://www.indiegogo.com/about/privacy>, Multifinanțare <http://multifinantare.ro/Home/TermsAndConditions>, accesate 12.11.2018.

³³ Kickstarter Privacy Policy: “When we share data with third-party services that support our delivery of the Kickstarter Services, we require that they use your information only for the purposes we’ve authorized, and that they protect your personal information at least to the same standards we do.”, [Online] la <https://www.kickstarter.com/privacy?ref=global-footer>, accesat 12.11.2018.

³⁴ *Crowdfunding site Kickstarter says hackers breach user data*, CBS News, [Online] la <https://www.cbsnews.com/news/kickstarter-customer-data-breach-hackers/>, accesat 12.11.2018.

îngrijorare este faptul că în anul 2017, informațiile sustrase de atacatori au fost făcute publice³⁵.

În final, provenind din delocalizarea geografică a *crowdfunding*-ului, care a fost facilitată de dezvoltarea instrumentelor de tranzacții online la distanță, problema juridică a riscului asociat cu spălarea banilor și finanțarea terorismului merită de asemenea menționată. Pentru a lupta împotriva acestui risc, țări precum Statele Unite ale Americii au adoptat noi reglementări exprese pentru platformele de *crowdfunding*, obligându-le la implementarea unor măsuri anti-fraudă cel puțin prin monitorizarea tranzacțiilor³⁶.

Problema în discuție a fost semnalată și de Autoritatea europeană pentru valori mobiliare și piețe – European Securities and Markets Authority (ESMA), care a susținut că finanțarea participativă bazată pe investiții prezintă un risc de abuz pentru finanțarea terorismului, mai ales atunci când platformele efectuează o procedură de *due diligence* limitată sau nu efectuează deloc o astfel de procedură cu privire la titularii de proiecte și la proiectele acestora, pentru a verifica dacă, în mod deschis sau în secret, se colectează fonduri pentru finanțarea teroriștilor³⁷. În aceste condiții, propunerea de Regulament la nivelul UE, prin articolul 9, impune ca plățile pentru tranzacțiile de finanțare participativă să aibă loc prin intermediul unor entități autorizate în conformitate cu Directiva (UE) 2015/2366 privind serviciile de plată (DSP) și care, prin urmare, intră sub incidența celei de-a patra directive privind combaterea spălării banilor, indiferent dacă plata este realizată de platformă sau de o parte terță. Articolul 9 prevede, de asemenea, că furnizorii de servicii de finanțare participativă trebuie să se asigure că titularii de proiecte acceptă oferte de finanțare participativă sau orice plată numai prin intermediul unei entități autorizate în temeiul DSP.

3. Concluzii

³⁵ N. Douglas, Info From 15 Million Breached Kickstarter and Bitly Accounts Is Now Publicly Available, [Online] la <https://lifelifehacker.com/15-million-hacked-kickstarter-and-bitly-passwords-are-n-1819216049>, accesat 12.11.2018.

³⁶ Titlul III – “Crowdfunding” din *Jumpstart Our Business Startups Act (JOBS Act)*, [Online] la <https://www.gpo.gov/fdsys/pkg/BILLS-112hr3606enr/pdf/BILLS-112hr3606enr.pdf>, accesat 12.11.2018.

³⁷ European Securities and Markets Authority, *Questions and Answers: Investment-based crowdfunding: money laundering/terrorist financing*, [Online] la https://www.esma.europa.eu/sites/default/files/library/2015/11/esma_2015_1005_qa_crowdfunding_money_laundering_and_terrorist_financing.pdf, accesat 12.11.2018.

În adaptare constantă pentru a ține pasul cu ultimele inovații de pe piața FinTech și pentru a putea reduce riscul breșelor de securitate asociat tranzacțiilor online, activitatea platformelor de *crowdfunding* este în prezent în plină dezvoltare. Creșterea numărului acestora, diversificarea serviciilor oferite și, mai ales, sporirea considerabilă din ultimii ani a numărului de utilizatori și a sumelor tranzacționate între aceștia, au transformat platformele în ținte propice atacurilor informatice.

În așteptarea unor intervenții legislative care să prevadă obligații suplimentare în sarcina furnizorilor de servicii de finanțare participativă în sensul asigurării unui nivel înalt de securitate în folosirea platformei, precum și prin reglementarea modalităților de control al îndeplinirii acestor obligații, pentru protejarea drepturilor lor, utilizatorii își pot lua o serie de măsuri rezonabile și pot manifesta prudență, recomandată, de altfel, în opinia noastră, pentru orice tranzacții online, fie ele de bani sau de date, fie prin intermediul platformelor de *crowdfunding* sau al altor platforme.

