CYBERLAW

by CIJIC

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente.***

CYBERLAW by CIJIC

EDIÇÃO N.º XI – MARÇO DE 2021

REVISTA CIENTÍFICA SOBRE CYBERLAW DO CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO – CIJIC – DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

CYBERLAW
by CIJIC

EDITOR: NUNO TEIXEIRA CASTRO

SUPORTE EDITORIAL: EUGÉNIO ALVES DA SILVA e AFONSO FREITAS DANTAS

PRESIDENTE DO CIJIC: EDUARDO VERA-CRUZ PINTO

COMISSÃO CIENTÍFICA:

- ALFONSO GALAN MUÑOZ

- ANGELO VIGLIANISI FERRARO

- ANTÓNIO R. MOREIRA

- DANIEL FREIRE E ALMEIDA

- ELLEN WESSELINGH

- FRANCISCO MUÑOZ CONDE

- MANUEL DAVID MASSENO

- MARCO ANTÓNIO MARQUES DA SILVA

- MARCOS WACHOWICZ

- ÓSCAR R. PUCCINELLI

- RAQUEL A. BRÍZIDA CASTRO

CIJIC: CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

ISSN 2183-729

CYBERLAW by CIJIC

NOTAS DO EDITOR:

Finda Março do ano de 2021.

Passou um ano desde que o mundo se confinou, massivamente. Fechados, em casa, nunca como a partir disto o acesso à *Internet* se nos desvelou como um direito humano fundamental.

O sonho de uma *internet* livre, neutral, aberta, inclusiva, universal será possível?

Provavelmente muitos de nós, que navegam por ela, num ou noutro canto de conversação e/ou *stop by* possível a partir de um dos nossos hodiernos cárceres físicos, já nos deparámos com um curioso grafo. Nele consta uma espécie de sondagem onde à pergunta: *"Quem fez mais pela digitalização da sua organização no último ano?"*, a percentagem do vencedor surpreende.

Não, não foi o CEO da organização. Também não, não foi o CISO (quando as organizações os têm). Sim, também não foi nenhum diretor de nenhum departamento da organização.

O principal responsável, sim, foi ela: a pandemia de covid-19.

É inegável. A pandemia acelerou o processo de digitalização de grande parte das interações humanas, sejam elas de qualquer natureza, escola, comércio, socialização.

Não obstante, por mais benefícios que este *input*, à *força bruta*, tenha trazido, a humanidade tem ainda um caminho muito longo para percorrer.

Num plano macro, que convoca a humanidade, combater ferozmente a exclusão digital, com particular enfoque nos reversos, *i.e.*, mais novos e mais velhos; sociedades desenvolvidas/mais pobres.

E se o acesso não é universal (sê-lo-á algum dia?), plural, em condições idênticas, inclusivo…também não deixará de ser preocupante, dentro daqueles que podem aceder, o número de indivíduos com falta de formação, com falta de um mínimo de educação/formação para usufruir da Rede.

Atente-se, porém, num plano micro, por exemplo, no caso português.

Entregue, neste último dia de Março de 2021, o RASI2020[1], nele despontam algumas evidências sobre a temática da falta de educação para o *ciber*. Os crimes praticados na e pela *Internet*, nomeadamente, *phishing*, *vishing*, *ransomware* e extorsão[2], em passo crescente, decorrem de variadas falhas ao nível do utilizador. Sobressai, da leitura crua dos números, uma inexistente cultura de ciberhigiene. A facilidade de promoção de engenharias sociais avulsas. É esta omissão de cibereducação responsável pela inabilidade em detetar o logro e burlões, em actividade fervorosa. No compasso da oferta/procura de produtos através do digital, se as trocas aumentam exponencialmente, paralela e em acompanhamento, as situações de fraude, burla, roubo, *Money mules*, etc., *idem*.

As múltiplas deficiências ao nível do utilizador – o famoso factor humano é implacável - e a violência de uma *digitalização à força bruta* de uma grande maioria das organizações, combinadas… dão razão de ser à *tame joke* informática de que, *na prática, em termos de ataques e crimes informáticos, só há dois tipos de organizações: as que*

1 Disponível para consulta em: https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNDQ1NAUABR26oAUAAAA%3d (último acesso 31MAR21)
2 *Vide* páginas 67 e ss do RASI2020.

sabem que já foram atacadas e as que ainda não o sabem (a premissa irónica é, infelizmente, igualmente válida para as pessoas singulares).

Torna-se inadiável que, paralelamente ao percurso do Direito no séquito da acelerada digitalização, as organizações, as pessoas, o Estado, entendam, decisiva e finalmente, a importância da segurança da informação[3].

Apaticamente, e em crise, as omissões perduram. Sedimentam.

Os alertas não chegam a bom porto. Provenham eles de serviços mais ou menos capacitados do Estado, sejam serviços secretos nacionais, sistema de segurança interna, observatórios…jaz, apenas, a constatação impotente de que "(…) *observa-se um aumento da espionagem através de ameaças persistentes, tecnologicamente avançadas, de origem estatal, direcionadas a importantes centros de informação do Estado. Uma das consequências da sofisticação enunciada, prende-se com a crescente dificuldade em destrinçar ataques informáticos para efeitos de crime económico ou de crimes de sabotagem, dirigidos a empresas e grupos de empresas com relevância no tecido empresarial nacional*."

No presente, de crescente digitalização, de cascata informacional, já todos sabemos que não é a quantidade de informação que serve à melhor tomada de decisão; é a qualidade. Mostra-se-nos angustiante o sublinhado de "*ameaças persistentes, tecnologicamente avançadas, de origem estatal, direcionadas a importantes centros de informação do Estado"*.

O Estado, como nunca, até como condição de promoção e prossecução geracional, tem o dever de defender um desígnio de soberania consubstanciado, precisamente, na superioridade informacional.

Conhecerá o Estado a capital importância da superioridade informacional?

Estará capacitado, humana e tecnologicamente, para proteger, o mais eficazmente possível, os seus mais valiosos *assets*, as suas infraestruturas mais críticas?

---

3 Ainda, no RASI2020 agora dado a conhecer, «(…) *No universo da ciberespionagem, registaram-se novos ciberataques contra infraestruturas críticas nacionais, com a finalidade de aceder a informação classificada, com valor político e económico."*», página 102.

Severa, a frieza dos parágrafos, no contexto pandémico Covid-19: "*No que concerne a outra das ameaças, i.e., as operações cibernéticas ofensivas, foram identificados agentes estatais e não estatais, visando entidades públicas e privadas, em particular no que respeitou à exploração de oportunidades…Verificaram-se inúmeros ciberataques registados contra instituições do setor da saúde, bem como operações de ciberespionagem contra entidades de investigação cientifica, particularmente envolvidas na pesquisa de terapêuticas e de vacinas contra a doença em apreço.*"

A segurança da informação, e a superioridade informacional que daí possa erigir, são, no contexto, de suma importância.

Infelizmente, as ameaças são múltiplas. Se, como veremos nesta nova edição, a Segurança da informação nas organizações(SiO) é tema fulcral, a erosão, de direitos fundamentais humanos, não descola de uma objetificação pronunciada da pessoa, do ser individual. Discreta, mas de forma expedita, as *oportunidades geradas pelo contexto pandémico*, têm servido para que o Estado arroje sistemas de videovigilância por múltiplas localidades nacionais[4]. A febre dos sistemas *CCTV* públicos segue a passo acelerado.

Em simultâneo, embora a aplicação *stayawaycovid* não tenha vingado, ainda, é certo que o controlo à distância da pessoa irá figurar, brevemente, em alguma medida legislativa. Notemos, ainda no contexto da pandemia, por exemplo, e em pleno estado de emergência, os níveis de mobilidade do cidadão. Com a proibição de circulação fora-do-concelho e a aproximação do tema festivo pascal, na semana de 25/26 de Março, acordámos com a notícia: "*Portugueses fogem para longe das restrições: um em cada dez dormiu a mais de 100 quilómetros de casa esta quinta-feira.*"[5].

4 Ainda no RASI2020, dentre renovações e novas autorizações, surgem destacadas 8 despachos de autorização de instalação de múltiplas cameras de videovigilância para localidades. Consultáveis a partir dos Anexos do relatório, Medidas legislativas, página 15 e ss.
Nota: entretanto, no início do mês de março 2021, foi-nos dada a conhecer a autorização para instalação de mais 216 cameras de videovigilância na cidade de Lisboa, para juntar às já existentes (o Bairro Alto já dispõe de sistema, por exemplo).

5 https://expresso.pt/sociedade/2021-03-26-Portugueses-fogem-para-longe-das-restricoes-um-em-cada-dez-dormiu-a-mais-de-100-quilometros-de-casa-esta-quinta-feira-b98a7df0 (último acesso 31MAR21).

A observação - próxima da realidade? - feita por uma consultora privada[6], revelando que mais de *um milhão de portugueses dormiu fora de casa*, curiosamente, não promoveu nenhum sobressalto jurídico. Nem social. A ordem continua serena. *Curiosamente*. Mas, não houve tratamento de dados pessoais para a revelação de tais estatísticas em mobilidade? Que finalidade jurídica prosseguiu a captura de tais dados? Que dados foram recolhidos? Foram coligidos de forma lícita? Que tratamento tiveram? Quais as garantias de anonimização e/ou minimização do tratamento?

Alguém questionou?

Alguém se indignou?

Não sendo a primeira vez que uma entidade privada analisa dados dos portugueses, em massa, sem qualquer tipo de reacção/oposição por parte destes, presumivelmente, como solução eficiente a tomar por parte do Estado, no futuro deveremos promover toda uma actividade concursal de fundos públicos para *investigação* - geral e abstrata - de *tendências*, *mobilidade*, *gostos e desejos* dos portugueses. Não que haja uma qualquer necessidade de uma finalidade concreta, lícita de sopeso. Afinal, o problema, de fundo, do sobressalto cívico e jurídico, da ordem, reside numa mera formalidade de *marketing*, o "publico não pode" vs. "privado tudo pode".

Acabemos prontamente com a folia[7].

O acesso a metadados são um problema para a acção das nossas secretas?

Do titular da acção penal, *tout court*, português?

---

6 Vejamos, por exemplo, o detalhe dos grafos sobre a evolução do confinamento e mobilidade em: https://www.pse.pt/evolucao-confinamento-mobilidade/ (último acesso 31MAR21).

7 Reparem na notícia: https://www.jornaldenegocios.pt/economia/impostos/amp/fisco-vai-ter-assistente-virtual-no-facebook-para-responder-as-duvidas-de-irs (último acesso 31MAR21).
Ora, a Autoridade Tributária portuguesa entende que a plataforma do Facebook é a melhor disponível *para tirar dúvidas a contribuintes nacionais.* Como todos sabemos, e somos *surpreendidos semanalmente*, o Facebook, provavelmente, já é conhecedor da informação fundamental e necessária dos seus utilizadores. Com este *passo de modernidade* da nossa AT, na prática, ao Facebook bastar-lhe-á agrupar a informação detida à contributiva, com os rendimentos declarados, das finanças portuguesas e... *Et voila*, vitracidade completa do cidadão. (quanto será o preço de cada miríade informacional de um contribuinte concreto que a AT poderá desembolsar? Haverá já um acordo bilateral entre a entidade privada e a AT?)
É, pois, tempo de assumirmos já a cedência gratuita dos nossos dados pessoais às entidades privadas e, a partir daí, o Estado seja profícuo no controlo de todas as nossas actividades sem qualquer tipo de sobressalto jurídico ou social.

Renunciemos à recolha de torrentes de dados pessoais às entidades privadas, assumamos a bonomia do *surveillance capitalism*, encapotando o próprio "*estado de vigilância*", e vivamos felizes.

E ordeiros. Sem sobressaltos.

A justificação, para esta aceitação social passiva e dócil, por parte de uma maioria de cidadãos, refletindo, denota muito do seu analfabetismo. Analfabetismo digital. Mas também social. A ordem das coisas apenas sobrepuja o ponto de partida. A liberdade individual é gratuitamente cedida a entidades privadas. Nunca ao Estado. A compressão de direitos fundamentais apenas terá de partir deste porto privado.

Aquiesçamos, afinal, mais de duzentos anos depois, a sociedade não compreende o ditame de que "*uma sociedade que troca um pouco de liberdade por um pouco de ordem acabará por perder ambas, e não merece qualquer delas*"[8].

Nesta nova edição da Cyberlaw by CIJIC, em consonância com os docentes do Mestrado em segurança da informação e direito do ciberespaço[9], tivemos o ensejo de provocar alguns discentes a reflexões sobre a realidade pungente que convoca a sociedade. No presente e para o futuro. Entre a segurança da informação nas organizações (SiO), a consciencialização dos funcionários das organizações para a temática, o factor humano na SiO; dados pessoais em *Schrems II* e acesso a metadados por parte do MP sem um suspeito determinado ou determinável, *not/net neutrality*, os discentes procuraram reunir algumas interjeições que, como já demos conta oportunamente, ajudem a mitigar a desigual compreensão, a despertar a consciencialização individual para promoção de um combate ao analfabetismo digital.

Trazemos, também, a participação de proeminentes juristas brasileiros que acederam ao nosso convite para dissertarem sobre a lei geral de proteção de dados brasileira assim como sobre o fenómeno do *stalking* em contexto laboral inclusive em ambiente digital.

8 Thomas Jefferson (1743-1826), carta a James Madison.
9 https://fenix.tecnico.ulisboa.pt/cursos/msidc

Resta-me, assim e por fim, agradecer a todos quantos contribuíram para mais esta nova edição da Revista, pelo esforço, pela disponibilidade, pela obra, endereçando a todos, em nome do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa, um merecidíssimo: - Muito Obrigado.

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente*.**

Boas leituras.

Lisboa, FDUL, 31 de Março de 2021

Nuno Teixeira Castro

CYBERLAW by CIJIC

O FATOR HUMANO NA SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES: UM *CASE STUDY.*

MELISSA ADRIANA GONÇALVES DE SOUZA*

e

GONÇALO NUNO BAPTISTA DE SOUSA†

* Mestranda em segurança da informação e direito ciberespaço.
† Professor e investigador na Escola Naval.
Contacto: goncalobsousa@gmail.com

RESUMO

O presente estudo traz à reflexão os impactos do fator humano na segurança da informação nas organizações, tanto sob o aspecto positivo quanto no negativo. A problemática que se quis apresentar aqui não é apenas a fraqueza ou a falha humana, mas também o olhar curioso e crítico que apenas uma pessoa poderia ter sobre determinada operação ou processo dentro de uma empresa. A proposta do tema tem como origem o caso ocorrido com o Banco HSBC após a aquisição do Banco Bital (México) dando-se foco na contribuição humana não apenas na concretização da fraude, mas principalmente na sua resolução, o que nos leva a concluir que a segurança da informação nas organizações tem grande relação com pessoas: O fator humano.

Palavras-Chave: Informação, segurança da informação, fator humano, engenharia social e vulnerabilidades.

ABSTRACT

The present study brings to reflection the impacts of the human factor on information security in organizations, both from a positive and a negative aspect. The problem that we´d like to present here is not only about human weakness or failure, but also the curious and critical look that only one person could have on a particular operation or process within a company. The focus of this study was based on the case that occurred with HSBC Bank after the acquisition of Bital Bank (Mexico), focusing not only on human contribution to prevent fraud, but mainly in its resolution, which leads us to conclude that information security in organizations has a strong linked with people: the human factor.

Keywords: Information, information security, human factor, social engineering and vulnerabilities.

1.INTRODUÇÃO

O tema proposto é uma junção de assuntos relativos ao conteúdo aprendido nas aulas de Segurança da Informação na Organizações (SIO) ministradas pelo Professor Dr. Gonçalo Sousa no curso de Mestrado em Segurança da Informação e Direito no Ciberespaço (MSIDC) e da experiência vivenciada na minha atuação profissional junto ao banco HSBC Bank Brasil S.A. entre os anos de 2014 a 2016.

Em 2010, o banco HSBC (subsidiária do México) foi acusado pelo senado norte americano por possuir um sistema de monitoramento e controle de operações financeiras pouco eficiente na prevenção à lavagem de dinheiro, indicando que isso acarretou na exposição do sistema financeiro dos Estados Unidos (EUA) a uma ampla rede de lavagem de dinheiro, tráfico de drogas e financiamento ao terrorismo. Ainda, o senado americano afirma que foram mais de 28 mil transações irregulares realizadas pelo HSBC durante o período de 2001 a 2008. Há indicação que o Irão estaria envolvido em 25 mil dessas movimentações que envolveram cerca de 19,4 mil milhões de dólares.

Em 2012, o HSBC fez um acordo com o departamento de Justiça dos Estados Unidos, comprometendo-se a pagar aproximadamente dois mil milhões de dólares, bem como fazer uma carta de confissão assumindo os erros cometidos pelo banco na falta de monitoramento adequado das suas operações, e também firmou o compromisso público de reforçar seu sistema de alertas e de investigações internas, não podendo pelos próximos 5 anos (2012 a 2017) incorrer em nova fraude de qualquer de suas filiais sob pena de perder a licença de atuar como instituição financeira nos Estados Unidos[1].

A questão que se quer trazer a análise neste trabalho é como o fator humano pode interferir na segurança da informação nas organizações tanto no aspecto positivo quanto no aspecto negativo. A problemática que se quer abordar não é apenas a fraqueza ou a

1 Disponível em: https://www.justice.gov/opa/pr/hsbc-holdings-plc-and-hsbc-bank-usa-na-admit-anti-money-laundering-and-sanctions-violations acesso em 07/01/2021.

falha humana, mas também o olhar curioso e crítico que apenas um humano poderia ter sobre determinada operação ou processo dentro de uma empresa.

Importante dizer em primeiro lugar, e isso será abordado de forma mais aprofundada ao longo deste trabalho, que o fator humano foi ao meu ver, no caso do HSBC, a peça chave tanto no que se pode dizer do aspecto negativo, ou seja, na concretização das fraudes, mas também no apontamento da questão e da resolução do problema, ainda que de forma a expor um instituição a um risco reputacional mundial. Em segundo lugar é salutar destacar que os fatos aqui apresentados são públicos e não estão amparados por nenhuma forma de sigilo, de forma que não há óbice em expor tais acontecimento neste estudo, além de vários jornais ao redor do mundo terem publicados os fatos acorridos, o caso virou um documentário da *Netflix*[2].

2 A *Netflix* reconta a história da fraude no HSBC no documentário intitulado "Na Rota do Dinheiro Sujo", episódio: "O banco dos carteis". Para recontar a história do banco a Netflix convidou várias pessoas que, na época, participaram de alguma forma com a investigações dos fatos, como por exemplo: 1) Everett Stern, ex-funcionário do HSBC (Compliance Officer do HSBC entre os anos de 2010 e 2011); 2) Anabel Hernandéz, jornalista investigativa e escritora; 3) William Ihenfeld, Procurador-geral em Virginia Ocidental (2010 a 2016); 4) Brett Wolf, Jornalista correspondente sobre Prevenção à lavagem de dinheiro para o Thomson Reuters; e 5)Matt Taibbi, jornalista correspondente da Rolling Stone magazine.

2. Segurança da Informação nas Organizações

Quando falamos em segurança da informação nas organizações inevitavelmente vem-nos à mente a ISO 27001, que é uma norma padrão internacional de referência no tema. Segundo o portal informativo da ISO 27001[3] a adesão da norma "*serve para que as organizações adoptem um modelo adequado de estabelecimento, implementação, operação, monitorização, revisão e gestão de um Sistema de Gestão de Segurança da Informação*".

Sabemos que a segurança da informação nas organizações envolve um conjunto de requisitos, processos e controles para mitigar riscos e isso impacta de várias formas dentro de uma empresa: como as telecomunicações, segurança aplicacional, proteção do meio físico, recursos humanos, continuidade de negócio, confiabilidade da marca, licenciamento, etc.[4].

Conceitualmente a segurança da informação está baseada na tríade "CIA" (sigla em inglês para *Confidentiality*, *Integrity* and *Availability*[5]): confidencialidade, integridade e disponibilidade das informações.

A confidencialidade está relacionada aos mecanismos de segurança que são adotados pela empresa para evitar que informações sensíveis sejam expostas, seja por meio de ciberataques, espionagem, fraudes, ou quaisquer outras práticas indevidas. Já a integridade refere-se à confiabilidade das informações e sistemas no decorrer do ciclo de vida dos dados, é a manutenção do armazenamento dos dados sem que qualquer interferência possa corrompê-los ou danificá-los. Enquanto que a disponibilidade está diretamente relacionada ao acesso às informações, ou seja, as informações devem estar disponíveis para serem consultadas a qualquer tempo por seus colaboradores, por exemplo[6].

---

3 Disponível em: https://www.27001.pt/iso27001_2.html acesso em 20/12/2020.
4 Disponível em: https://www.27001.pt/index.html acesso em 20/12/2020.
5 Disponível em: https://www.techrepublic.com/blog/it-security/the-cia-triad/ acesso em 21/12/2020.
6 Disponível https://www.telium.com.br/blog/confidencialidade-integridade-e-disponibilidade-os-tres-pilares-da-seguranca-da-informacao.

Nesta perspectiva podemos observar que é notória a importância da segurança da informação para que as organizações mantenham seus sistemas protegidos, não apenas pela relevância das informações internas ou de seus clientes, ou ainda pela questão reputacional, mas principalmente para a continuidade dos seus negócios.

Sabemos também que há várias formas de ataque à segurança da informação de uma organização como por exemplo: vírus[7], vulnerabilidades dos *softwares*[8]; ciberataques[9], *fishing*[10], *spam*[11], engenharia social[12], entre outros.

Para resumir:

> "*A segurança de informação é o processo de proteger a informação de diversos tipos de ameaças internas e externas que coloquem em risco a continuidade do negócio e o retorno dos investimentos feitos. A adopção e implementação de um sistema de segurança é uma decisão particular de cada organização que é influenciada pelas necessidades e objectivos da empresa, requisitos de segurança, capital investido, tamanho e estrutura da organização. Assim sendo deve ser feita uma*

---

7 CORTEZ, Igor Siqueira e KUBOTA, Luis Claudio. Contramedidas em segurança da informação e vulnerabilidade cibernética: evidência empírica de empresas brasileiras. 2021, pág. 759. Disponível em: https://www.researchgate.net/profile/Luis_Kubota/publication/259360942_Contramedidas_em_seguranca_da_informacao_e_vulnerabilidade_cibernetica_evidencia_empirica_de_empresas_brasileiras/links/00b7d52b31b2030da9000000/Contramedidas-em-seguranca-da-informacao-e-vulnerabilidade-cibernetica-evidencia-empirica-de-empresas-brasileiras.pdf. Acesso em 08/12/2020.

8 Idem pág. 3.

9 Os Ciberataques como um Novo Desafio para a Segurança: o Hacktivismo. 2015 pág. 42. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/15403/1/Disserta%C3%A7%C3%A3o%20de%20mestrado%20Final%20Elisabete%20Domingues.pdf acesso em 12/12/2020.

10Miller, Andrew. Phishing: An Insidious Threat to Financial Institutions. 2006. https://www.bankinfosecurity.com/phishing-insidious-threat-to-financial-institutions-a-121 acesso em 22/12/2020.

11 SILVA, Thiago Domingos de Souza. Segurança na Internet: Qual a nossa Vulnerabilidade? Pág 2. Disponível em: http://www.periodicos.letras.ufmg.br/index.php/ueadsl/article/viewFile/2603/2551 acesso em 07/12/2020

12 Engenharia social definição: "*Any act that influences a person to take an action that may or may not be in their best interest.*" *We have defined it in very broad and general terms because we feel that social engineering is not always negative, but encompasses how we communicate with our parent, therapists, children, spouses and others*.
Tradução livre: "*Qualquer ato que influencie uma pessoa a realizar uma ação que pode ou não ser de seu interesse". Definimos de uma forma geral porque achamos que a engenharia social nem sempre é negativa, mas abrange a forma como nos comunicamos com nossos pais, terapeutas, filhos, cônjuges e outros*. Disponível em: https://www.social-engineer.org/about/ acesso em 02/01/2021.

> *análise de risco que identifique as potenciais ameaças, apontando soluções que as eliminem, minimizem ou as transfiram a terceiros*"[13].

Ainda, sobre as ameaças internas à segurança da informação há dados estatísticos que mostram que a engenharia social é um dos fatores de risco que afeta mais de metade das violações a dados ocasionadas por ameaças internas:

> "*De acordo com a verizon (2016) foram encontrados indicadores estatísticos interessantes sobre as novas tendências de crimes informáticos, que mostram que a nova geração de ataques está a utilizar o factor humano para desencadear com frequência ataques a TI sem o uso de meios electrónicos*"[14].

Neste estudo o que se quer analisar é o fator humano como decisivo para o sucesso ou para o fracasso dos mecanismos de segurança da informação nas organizações. Para tanto, traz-se a análise o caso do banco HSBC que em 2010 foi acusado pelo senado norte-americano de não ter um sistema interno eficiente no controle das suas operações, acarretando a exposição do sistema bancário mundial à lavagem de dinheiro e financiamento ao terrorismo, e ao tráfico de drogas. Assim, a seguir apresenta-se um breve resumo dos fatos públicos[15] ocorridos naquela instituição financeira.

13 TAVARES, Telma Kidy da Conceição. O Fator Humano na Segurança de Informação nas Organizações. 2017. Pág 12.

14 TAVARES, Telma Kidy da Conceição. O Fator Humano na Segurança de Informação nas Organizações. 2017. Pág 4.

15 Todos os dados ou informações aqui apresentadas foram retirados de fontes públicas de consulta online e gratuita disponível na *internet* e para todas as informações são apresentadas suas fontes de pesquisas em notas de rodapé ou no próprio corpo do texto. Não foram utilizadas informações privilegiadas de dentro da instituição, com exceção da minha percepção pessoal sobre o tempo em que atuei profissionalmente naquela instituição (2014 a 2016) a qual faço menção unicamente no ultimo parágrafo das 'considerações finais' deste trabalho.

3. O *Case Study*

Tudo começou em 2012 quando a subsidiária do banco inglês HSBC (Hong Kong and Shanghai Banking Corporation) sediada no México foi acusada de lavar dinheiro para os cartéis de drogas. Esta foi a conclusão do relatório produzido pelo senado norte americano, que indica que milhares de milhões de dólares oriundo do narcotráfico e do terrorismo foram inseridos no sistema financeiro dos Estados Unidos da América por falha na operação do HSBC.

O senador Carl Levin que presidiu a subcomissão emissora do relatório afirmou que o banco possuía uma cultura "contaminada" e por isso permitiu que clientes recebessem valores de países de origem duvidosas como: Irão, Ilhas Cayman, Arábia Saudita e Síria[16].

Para entendermos como tudo isso aconteceu, é preciso voltar aos anos de 2002 quando o HSBC adquiriu a operação do Banco Bital no México, que na época era considerado o quinto maior banco do México[17] e foi adquirido por 1,14 mil milhões de dólares. O Bital com grande presença no México, principalmente em Sinaloa que é uma região conhecida por produção de narcóticos.

Juntamente com a aquisição das operações do Bital o banco HSBC "comprou" também os funcionários, os clientes e suas contas bancárias. O documentário da *Netflix*[18] que reconta essa história, com a participação de alguns dos personagens que participaram das investigações na época (ex-executivo do banco HSBC, procuradores de justiça e jornalistas investigativos)[19], indica que junto com aquisição o banco comprou inevitavelmente, contas bancarias dos narcotraficantes, bem como colaboradores

16 Disponível em: https://www.bbc.com/mundo/noticias/2012/07/120717_hsbc_escandalo_claves acesso em 10/01/2021.
17 Disponível em https://www.nytimes.com/2002/08/22/business/hsbc-buying-fifth-largest-bank-in-mexico-for-1.1-billion.html acesso em 10/01/2021.
18 O documentário da Netflix reconta a história da fraude no HSBC: "Na Rota do Dinheiro Sujo" Nome do episódio: "O banco dos carteis".
19 Pessoas que participaram das investigações dos fatos narrados na séria da Netflix (vide nota de rodapé n. 4): 1) Everett Stern, ex-funcionário do HSBC (Compliance Officer do HSBC entre os anos de 2010 e 2011); 2) Anabel Hernandéz, jornalista investigativa e escritora; 3) William Ihenfeld, Procurador-geral em Virginia Ocidental (2010 a 2016); 4) Brett Wolf, Jornalista correspondente sobre Prevenção à lavagem de dinheiro para o Thomson Reuters; e 5)Matt Taibbi, jornalista correspondente da Rolling Stone magazine.

corruptos que “facilitavam” a inclusão do dinheiro oriundo do narcotráfico no sistema bancário. Como o HSBC é um banco mundial, o dinheiro dos carteis passava naquele momento a ser inserido no sistema financeiro mundial.

Os jornais ao redor do mundo começaram a noticiar a falha nas operações do banco:

> “*O banco britânico HSBC expôs o sistema financeiro dos Estados Unidos a uma ampla rede de lavagem de dinheiro, tráfico de drogas e financiamento de terroristas devido ao seu fraco sistema de controle, diz um relatório do Senado dos Estados Unidos que investigou as filiais do banco no país por um ano*”[20].

Em 2010 o escritório regulador do banco federal americano “OCC” (Sigla inglesa para: “*Office of the Comptroller of the Currency*”[21]), solicitou ao HSBC que realizasse maior controle nas suas operações, foi por isso que naquele mesmo ano o HSBC estabeleceu em Delaware/USA um escritório para monitoramento dos alertas das operações financeira.

Importante dizer que nos Estados Unidos está em vigor a Lei do Sigilo Bancário “BSA” (sigla em inglês para *Bank Secrecy Act*), também conhecida como Lei Anti-Lavagem de Dinheiro “AML” (sigla em inglês para *Anti-Money Laundering*), e com isso todas as instituições financeiras com atuação naquele país devem manter registros detalhados e relatar às autoridades nacionais quaisquer atividades suspeitas que possam indicar lavagem de dinheiro ou quaisquer outros crimes que detectem em suas operações.

Fazem parte destes alertas monitorar e impedir operações com empresas, bem como com os países que compõe a lista de restrições do governo norte-americano. O escritório governamental de controle de ativos estrangeiros “OFARC” (sigla em inglês para “*the Office of Foreign Assets Control*") que é uma divisão do Departamento do Tesouro dos Estados Unidos que administra e aplica sanções econômicas e comerciais com base na política estrangeira do país e metas nacionais de segurança contra determinados países e regimes políticos, terroristas, traficantes internacionais de drogas, pessoas envolvidas em

---

20 Disponível em: https://www.correiocidadania.com.br/colunistas/consciencia-negra/33-artigos/noticias-em-destaque?start=924 acesso em 10/12/2020.
21 Site: https://www.occ.treas.gov/

atividades relacionadas com a proliferação de armas de destruição em massa e outras ameaças à segurança nacional, à política estrangeira ou à economia dos Estados Unidos.

Por isso, algumas sanções se aplicam de forma ampla a determinadas regiões (como Cuba e Irão), enquanto outras são direcionadas e concentradas em pessoas e entidades específicas[22]. Todas as restrições, impedimentos estão disponíveis no site Tesouro Nacional Norte-americano[23] para consulta.

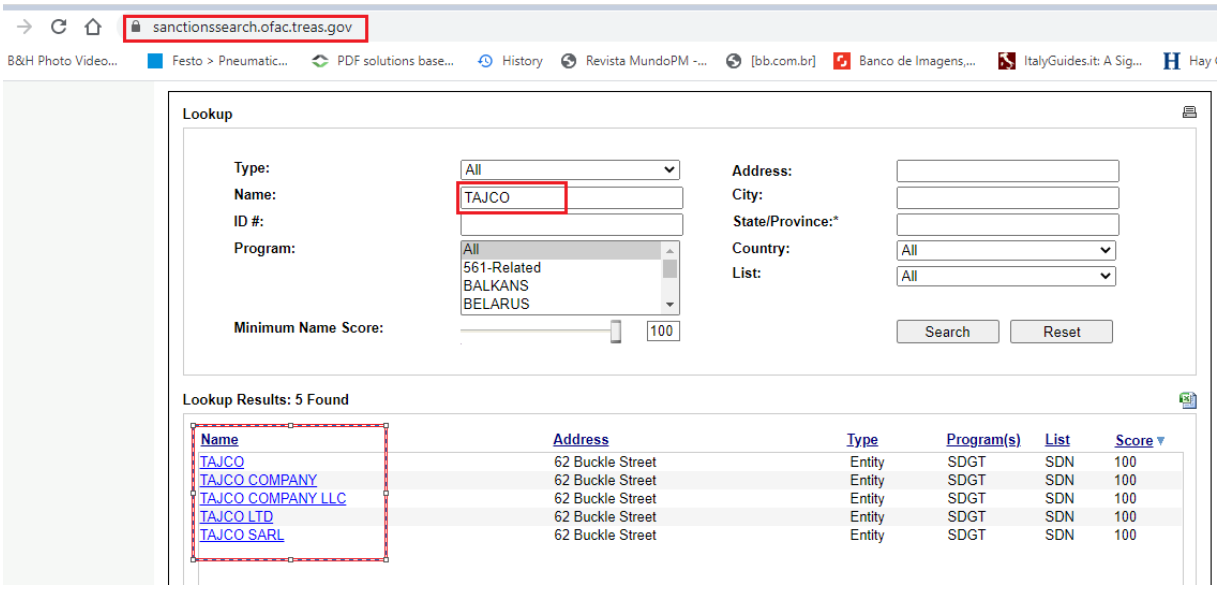
Por conta desta leis e regulamento o HSBC, assim como qualquer outro banco com operação naquele país, precisava verificar suas operações financeiras e reparar os problemas que foram apontados pelo OCC, o qual indicava que o sistema de monitoramento do banco como fraco e precisava ser reforçado, e foi para cumprir essas exigência que em 2010 um escritório em Delaware foi criado pelo HSBC.

Para esse escritório o HSBC contratou vários executivos e vários consultores, entre eles Everett Stern, executivo do banco que atuou como compliance officer do HSBC entre os anos de 2010 a 2011.

O trabalho de Stern, assim como de outras pessoas que foram trabalhar no mesmo escritório era 'limpar os alertas' gerados pelo sistema do banco. Os sistemas do banco estavam parametrizados conforme as diretrizes da OFARC e qualquer operação que fosse incompatível com essas regras, geravam alertas.

Por exemplo, se consultarmos a empresa "TAJCO[24]" na lista de pessoas com impedimento de realizar operação financeira com os Estados Unidos da América, encontraremos[25]:

22 Disponível em: https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information acesso em 11/12/2020.
23 Disponível em: https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list-data-files acesso em 12/12/2020.
24 Exemplo utilizado pelo Compliance Officer do HSBC na série da Netflix para explicar como o fator humano interfere na segurança da informação.
25 Lista de consulta pública disponível em: https://sanctionssearch.ofac.treas.gov/ acesso em 20/01/2020.



No *print* acima, destacado em vermelho, é possível verificar que na lista da OFARC aparecem todos as empresas com o nome 'TAJCO' que possuem restrições de realizar operações financeiras através dos sistema bancário norte-americano.

Assim, sempre que houver uma operação qualquer, envolvendo uma das empresas que esteja na lista de restrições, o sistema gera um alerta. O HSBC tinha um acúmulo muito grande destes alertas e este foi o motivador da estruturação do escritório em Delaware, era preciso "limpar" os alertas gerados, mas isso não queria dizer que o banco está agindo certo, mas ao menos estavam tentando agir corretamente.

O depoimento de Stern à *Netflix* indica que as pessoas que ali estavam a trabalhar não se mostravam interessadas a fazer o certo, estavam fazendo um trabalho sem realmente entender o que faziam. Stern descobriu várias transações realizadas as empresas que estavam na lista de restrições da OFARC e que haviam sido aprovadas pelo HSBC, o que estava errado. Ainda, Stern afirmou que o seu propósito de vida é "fazer o bem" indicando que queria "ter uma vida com um propósito e servir meu país e ser um instrumento para o bem e ser capaz de servir a um propósito maior" e assim três semanas após iniciar seu trabalho como executivo do HSBC começou a reportar as irregularidades à CIA (*Central Intelligence Agency of USA*).

O que Stern detectou como irregular nas operações realizadas no HSBC é que empresas, sancionadas ou banidas de realizarem operações financeiras com os EUA pela OFARC poderiam estar utilizando as fragilidades do sistema bancário para enviar dinheiro, por exemplo, a empresa 'TAJCO' que por sua vez poderia estar enviando dinheiro para o Hezbollah ou para Al Queda ou qualquer outra organização criminosa que estivesse listada pela OFARC.

A pergunta é como isso poderia acontecer se os sistemas do HSBC estavam parametrizados conforme as normas da OFARC? O que acontecia, segundo Stern, era que funcionários do HSBC faziam alterações dos nomes das empresas sancionadas ou banidas pela OFARC para manipular os sistemas do banco e possibilitar a remessa ilegal de dinheiro para terroristas e carteis de drogas.

Assim o que acontecia de forma mais específica, era que as operações que deveriam ser direcionadas a empresa "TAJCO" (nome que constava no sistema de restrições do banco) e assim seriam operações automaticamente negadas pelo sistema do banco, passam por manipulação humana e os nomes das empresas que apresentavam alguma restrição pela OFARC tinham seus nomes alterados de forma a burlar o sistema para por exemplo: "TAJ.CO" ou "T.A.J.C.O" ou ainda "TAJ/CO" e assim o sistema não detectava a irregularidade ou ainda quando detectava e gerava o alerta que eram tratados, também segundo Stern, por funcionários não comprometidos com suas atividades ou que não sabiam exatamente o que estavam a fazer.

Assim, com os reportes de Stern à CIA, iniciou-se uma investigação sobre os fatos que posteriormente levou o senado norte-americano a criar uma subcomissão para avaliar a conduta do HSBC, alegando que o banco estava usando suas filiais do México para lavar dinheiro, e fornecer dólares e acesso ao sistema financeiro dos EUA aos dos carteis de drogas, terrorismos. As investigações se forcaram nas negligencias do HSBC entre os anos de 2006 e 2009.

Em dezembro de 2012 o Banco HSBC fez um acordo com as autoridades norte-americanas que resultou no pagamento de valores da ordem de aproximadamente dois mil milhões de dólares. Ainda fazia parte do acordo a elaboração de uma carta de confissão pelos erros do banco e pela fraca gestão do monitoramento das suas operações e por último firmaram um compromisso público de reforçar o sistema de alertas e de

investigações internas, não podendo o HSBC (headquarter ou qualquer uma de suas filiais) pelos próximos 5 anos (2012 a 2017) incorrer em novas fraudes sob pena de perder a licença bancária de atuar como instituição financeira nos Estados Unidos[26].

4. O fator Humano na Segurança da Informação nas Organizações

Analisando os fatos acima é possível concluir que, no caso que envolveu o HSBC, não faria diferença quantos mil milhões de dólares o HSBC investiu em sistemas de segurança para fortalecer e garantir a legalidade das suas operações, a fraude continuaria a acontecer, pois o fator humano era a principal falha de toda a sua operação. Na lição de Kevin Mitnick:

> "*Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável*"[27].

A vulnerabilidade do fator humano nas organizações pode acontecer de várias maneiras, isso porque as motivações do ser humano, as emoções de cada um são muito variáveis e difíceis de prever, monitora ou evitar:

> "*O maior problema na segurança são as pessoas, que pelas suas características psicoemocionais podem facilmente serem manipuladas, induzidas, coagidas, ou forçadas a violar aspecto de segurança para conceder acesso ou privilégios a alguém, daí que, a*

26 Disponível em: https://www.justice.gov/opa/pr/hsbc-holdings-plc-and-hsbc-bank-usa-na-admit-anti-money-laundering-and-sanctions-violations acesso em 07/01/2021.

27 Ob. Cit. TAVARES, Telma Kidy da Conceição. O Fator Humano na Segurança de Informação nas Organizações. 2017. Pág. 03. In Mitnick & Simon (2002), p.15. – (Mitnick, K.& Simon, W.(2002). The art of deception: Controlling the human element of security. New York. John Wiley & Sons).

> *maior protecção contra a Engenharia Social, continua a ser a educação e consciencialização*"[28].

As informações confidências de uma empresa, incluindo aqui as possíveis falhas de sistemas operacionais, podem ser obtidas de várias maneiras, como a manipulação psicológica de funcionários[29], coação, ameaças que posteriormente servirão para concretização da fraude.

No caso em tela, podemos verificar o fator humano atuando tanto no aspecto negativo, quanto no positivo:

O sentido negativo da atuação humana no caso do HSBC pode ser destacado na atuação humana que permitiu a execução da fraude interna, tendo em vista o conhecimento que se tinha sobre as falhas no sistema e de como burlá-las. O documentário da Netflix menciona, mas não há evidências que possam confirmar tal alegação no sentido de que muitos funcionários do Banco Bital eram corruptos e com a aquisição pelo HSBC esses funcionários corruptos agora tinham acesso ao sistema financeiro de um banco mundial, o que possibilitava a remessa de dinheiro ilegal para qualquer lugar do mundo. Ainda, também há indicação de que os cartéis de drogas do México usavam de coações físicas e morais, bem como valiam-se de ameaças constantes aos funcionários do Bital/HSBC, sinalizando que a sua integridade física e de suas famílias estariam comprometidas se não tivessem o apoio necessário para a realização das transações financeiras fraudulentas ou ilegais.

Soma-se a isso, ainda dentro do fator humano nas organizações, por afirmação do ex- executivo do HSBC (Stern) muitos funcionários do escritório do HSBC em Delaware, que foram contratados para "limpar" os alerta gerados pelos sistemas de detecção de fraude do banco, não estavam cientes da importância das suas atividades ou simplesmente não sabiam o que estavam a fazer.

Mas, ainda analisando o mesmo caso do banco HSBC (acusado de fraude contra o sistema financeiro, que pagou uma multa de quase dois mil milhões de dólares, e que também confessou a pratica de algumas práticas ilegais), há também o fator humano no

28 TAVARES, Telma Kidy da Conceição. O Fator Humano na Segurança de Informação nas Organizações. 2017. Pág 22.
29 Idem pág. 67.

seu aspecto positivo, que pode ser creditado a atitude, e ao olhar atento do ex-excutivo do banco que tinha como lema de vida “fazer o bem”, ou seja, a motivação deste colaborador era fazer a coisa certa, e assim conseguiu, com ajuda da CIA, dos procuradores gerais e demais autoridades envolvidas nas investigações, descobrir, interromper e corrigir uma falha interna do sistema bancário do banco HSBC.

5. Considerações Finais

Assim, após a análise do presente caso, que envolveu o banco HSBC México, com foco na contribuição humana tanto para a concretização da fraude, quanto para a resolução do problema, podemos afirmar que a segurança da informação nas organizações tem grande relação com pessoas: fator humano. Ainda que seja possível verificar que a maioria das empresas direcionam maior importância aos processos, software ou tecnologia para manter a segurança das informações, visto que os maiores investimentos são destinados a essas frentes.

A questão que poderia ser colocada aqui é: Para evitar fraudes internas, como a que aconteceu com o HSBC após a aquisição do Banco Bital, é necessário reduzir a interação do ser humano com processos relativos à segurança da informação? Nesse sentido, merece um alerta sobre este tema para que as empresas direcionem esforços (de tempo, de investimento, de capacitação) as questões relativamente aos processos de segurança da informação que envolvam pessoas, o que pode ser feito, por exemplo, estabelecendo políticas, normas e procedimentos de segurança da informação, bem como treinamentos de seus colaboradores de acordo com o nível académico e de atuação profissional de cada um.

É indispensável que as empresas conheçam suas vulnerabilidades e que proponham práticas para diminuir, atenuar ou reduzir riscos de exposição de seus negócios. Importante dizer que tudo isso é uma construção cultural que as empresas consolidam ao longo da sua existência focando sempre em boas práticas.

Por fim, gostaria de destacar a minha atuação profissional no HSBC Brasil, que se deu entre os anos de 2014 e 2016[30] como suporte consultivo criminal no departamento jurídico. A minha principal função era auxiliar as investigações internas com foco na prevenção a fraudes, bem como reportar as autoridades brasileiras qualquer irregularidade detectada fossem elas oriundas de fraude interna (provada por colaboradores) ou externas (clientes, hackers, estelionatos, etc.) sem qualquer filtro

30 Em 2016 o HSBC Bank Brasil S.A. – Banco Múltiplo foi adquirido pelo Banco Bradesco S.A. e deixou de ter atuação no mercado varejista brasileiro.

relativo a cargos, funções ou valores. Ainda, apenas a título ilustrativo naquela oportunidade seguíamos padrões rígidos de treinamentos relacionados as políticas de segurança da informação, prevenção a corrupção, suborno e lavagem de dinheiro, bem como sobre regras de monitoramento de fraudes internas.

6. Referência Bibliográficas

TAVARES, Telma Kidy da Conceição. O Fator Humano na Segurança de Informação nas Organizações. 2017. Disponível em: https://www.bbc.com/mundo/noticias/2012/07/120717_hsbc_escandalo_claves

CORTEZ, Igor Siqueira e KUBOTA, Luis Claudio. Contramedidas em segurança da informação e vulnerabilidade cibernética: evidência empírica de empresas brasileiras. 2021. Disponível em: https://www.researchgate.net/profile/Luis_Kubota/publication/259360942_Contramedidas_em_seguranca_da_informacao_e_vulnerabilidade_cibernetica_evidencia_empirica_de_empresas_brasileiras/links/00b7d52b31b2030da9000000/Contramedidas-em-seguranca-da-informacao-e-vulnerabilidade-cibernetica-evidencia-empirica-de-empresas-brasileiras.pdf.

MILLER, Andrew. Phishing: An Insidious Threat to Financial Institutions. 2006. https://www.bankinfosecurity.com/phishing-insidious-threat-to-financial-institutions-a-121

SILVA, Thiago Domingos de Souza. Segurança na Internet: Qual a nossa Vulnerabilidade? Disponível em: http://www.periodicos.letras.ufmg.br/index.php/ueadsl/article/viewFile/2603/2551

Sites

- https://comum.rcaap.pt/bitstream/10400.26/15403/1/Disserta%C3%A7%C3%A3o%20de%20mestrado%20Final%20Elisabete%20Domingues.pdf
- https://www.bbc.com/mundo/noticias/2012/07/120717_hsbc_escandalo_claves
- https://www.correiocidadania.com.br/colunistas/consciencia-negra/33-artigos/noticias-em-destaque?start=924
- https://www.justice.gov/opa/pr/hsbc-holdings-plc-and-hsbc-bank-usa-na-admit-anti-money-laundering-and-sanctions-violations

- https://www.social-engineer.org/about/
- https://www.nytimes.com/2002/08/22/business/hsbc-buying-fifth-largest-bank-in-mexico-for-1.1-billion.html
- https://www.occ.treas.gov/
- https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information
- https://sanctionssearch.ofac.treas.gov/
- https://www.27001.pt/iso27001_2.html
- https://www.techrepublic.com/blog/it-security/the-cia-triad/
- https://www.telium.com.br/blog/confidencialidade-integridade-e-disponibilidade-os-tres-pilares-da-seguranca-da-informacao