



REDE
TEMPO
BRASIL



Boletim do Tempo Presente - ISSN 1981-3384

Cibersegurança em gestão de museus no século 21 nas Humanidades Digitais

Janaina Cardoso de Mello^I

Resumo: Com a velocidade nas transformações tecnológicas no século XXI, informações da maioria das organizações públicas e privadas migraram de arquivos físicos para nuvens digitais. Lidar com essa realidade diante de invasões cibernéticas promovidas por *hackers* exige muito mais do que o recurso a uma equipe de Tecnologia da Informação (TI). As ameaças de segurança digital em museus e centros culturais requerem a formação em Humanidades Digitais dos profissionais dessas instituições. Adotam-se nesse artigo procedimentos metodológicos qualitativos de análise sistematizada de literatura da área e estudos de *cases* selecionados.

Palavras-chave: Cibersegurança; Museu; Humanidades Digitais

Cybersecurity in museum management in the 21st century in the Digital Humanities

Abstract: With the speed of technological transformations in the 21st century, information from most public and private organizations migrated from physical files to digital clouds. Dealing with this reality in the face of cyber intrusions by *hackers* requires much more than recourse to an Information Technology (IT) team. Digital security threats in museums and cultural centers require the training in Digital Humanities of the professionals of these institutions. This article adopts qualitative methodological procedures of systematized analysis of literature in the area and studies of selected cases.

Keywords: Cybersecurity; Museum; Hacker; Digital Humanities

Introdução

Em 16 de abril de 2015, o jornal *Chicago Tribune* anunciou “*National Museum of Mexican Art website taken over by hacker*”, ou seja, a *homepage* do Museu Nacional de Arte Mexicana foi hackeada por alguém que se identificava como “um muçulmano” fazendo a invasão em nome do Islã. Na página inicial da instituição, os usuários que desejavam navegar pelas informações das exposições, peças de arte digitalizadas e outras atividades culturais, foram recepcionados por uma música com ofensas à países como “*Israhell*”, além dos EUA, Irã, Índia e França. O Curador chefe do Museu, Cesareo Moreno, foi chamado, assim como a Equipe de Tecnologia da Informação (TI) e a polícia de Chicago. O Museu estava às vésperas de inaugurar um grande evento e essa invasão cibernética colocava em xeque a reputação da instituição e a captação de doações financeiras por parte de investidores externos. Era uma situação completamente nova para os gestores daquela instituição e ali, naquele momento, a gestão não sabia o que fazer a não ser esperar que a equipe de informática resolvesse aquele problema.^{II}

A falta de formação e informação à respeito de cibersegurança de muitos gestores de instituições culturais além de não antecipar medidas preventivas de segurança colaborativa, sobrecarrega os técnicos sem que muitas vezes ocorra um diálogo inteligível entre as duas partes, fragilizando o trabalho dos últimos que aplicam soluções gerais para espaços digitais e físicos com especificidades das Humanidades (Museologia, a História, a Sociologia, a Antropologias, as Artes, etc.) que alimentam museus, galerias, centros culturais, bibliotecas, arquivos, dentre outros.

No final da década de 1980, com a realização da conferência “*Digital Humanities*” (1989) organizada pela Association for Computers and the Humanities e da Association for Literary and Linguistic Computing^{III}, os debates em torno do percurso trilhado pelas sociedades em direção ao universo digital tem impactado a produção e divulgação de conhecimentos dos campos das Ciências Humanas e Sociais, Artes e Letras no âmbito das tecnologias computacionais.

Em 2010, com a divulgação do “Manifesto das Humanidades Digitais”^{IV} por ocasião do *ThatCamp* 2010, reafirmou a “transdisciplinaridade” que deve associar “os métodos, os dispositivos e as perspectivas heurísticas das ciências humanas e sociais, ao mesmo tempo em que mobiliza as ferramentas e perspectivas singulares abertas pela tecnologia digital”. O que significa ainda argumentar que a “incorporação dos saberes tradicionais às tecnologias computacionais” requer o movimento equivalente da “incursão dos saberes tradicionais no terreno do conhecimento tecnológico”^V, ou seja, historiadores, museólogos, geógrafos, antropólogos e demais pesquisadores devem aprender o funcionamento e os formatos de criação das tecnologias digitais.

Mas essas discussões ainda permanecem tanto no aspecto formativo (universidades) quanto profissional (exercício pleno em instituições) como teorias distantes da prática dos profissionais das humanidades que trabalham em museus, galerias, centros culturais etc. Há uma grande preocupação com a guarda digital da documentação museológica, a digitalização de acervos, serviços museais em rede, todavia, as ações sobre cibersegurança são executadas por empresas externas e sem a interação dos funcionários na elaboração e aplicação destas. Isso deixa tais espaços vulneráveis para os hackeamentos.

Com o incremento da Inteligência Artificial (IA), cada novo criminoso pode aumentar exponencialmente o número de ataques através do crescente uso da automação. Milhões de mensagens de *spam* em massa não solicitadas são enviadas por automação em um curto período. Assim, os ataques de *hackers* agora também são automatizados, com até 80 milhões de invasões todos os dias.^{VI}

Na era da “Grande Informação” tudo o que é produzido por seres humanos ou *Bots* (robôs no âmbito da IA) e circulado no mundo virtual gera rastros digitais e uma infinidade de dados cumulativos, uma vez que

A chamada “explosão da informação” do pós-segunda guerra não pode ser comparada, em volume e intensidade, com a revolução causada pela expansão dos computadores pessoais, da *internet* e dos *smartphones* no final do século XX e início do século XXI. Novas unidades de medida de informação (*megabyte*, *gigabyte*, *terabyte*, *petabyte*, *exabyte*, *zettabyte*, *yottabyte*) são criadas para expressar o crescente e exponencial aumento na produção mundial, num fenômeno também conhecido por *big data*.^{VII}

Hadnagy^{VIII} alerta para a existência de mais de 4.48 bilhões de *websites* indexados, não contabilizando aqueles existentes na “*dark web*” ou “*deep web*”. Pois se ao redor do mundo, houve a ampliação do uso de equipamentos tecnológicos como computadores pessoais, *smartphones* e outros serviços de IA, é necessário começar a prestar atenção nos protocolos de segurança de última geração com inovação e expansão ainda em curso.^{IX}

Passados cinco anos, dada as rápidas mudanças tecnológicas, talvez o leitor desse artigo possa argumentar que o hackeamento na plataforma digital do Museu Nacional de Arte Mexicana foi uma lição aprendida. Será?

Em maio de 2019, o Museu de Arte Asiática em San Francisco também foi alvo de uma invasão cibernética. Foi utilizado um *ransomware*, ou seja, um tipo de *malware* em que o *hacker* ameaça publicar ou bloquear o acesso aos dados da vítima, a menos que um resgate seja pago. A rede de TV ABC anunciou o episódio quando o museu se recusou a pagar o resgate.^X

Entre 2014 e 2015 o Serviço Europeu de Polícia (EUROPOL) ressaltou o fato de o cibercrime estar se tornando cada vez mais hostil. Em vez de subterfúgio e dissimulação no engano do usuário, se propaga uma tendência de crescente de agressão em muitos ataques cibernéticos e, em particular, na extorsão com *ransomware* ou ataques DDoS (*Distributed Denial of Service*). Isso aumenta o impacto psicológico do medo e da incerteza sobre as vítimas.^{XI}

Mas o que é um *hacker*? O uso inicial do termo data de meados dos anos de 1950 e início dos anos de 1960 entre os estudantes do Massachusetts Institute of Technology (MIT) que se divertiam com trotes e depois estendido ao uso de linhas telefônicas para ligações gratuitas. Com o passar do tempo, *hacker* era uma pessoa com grande conhecimento na área da informática e em contínuo aprendizado das tecnologias digitais em transformação. Com o surgimento de invasões digitais, *hacker* passou a ser associado pela mídia às atividades criminosas em rede.^{XII}

Há muita contestação desse último significado e um alerta sobre os distintos tipos de *hackers*: a) *White Hat* (hacker ético): especialista em segurança da informação. Presta auxílio às empresas para encontrar vulnerabilidades existentes em seus sistemas. Considerados “hackers do bem”; b) *Black Hat* (hacker mal-intencionado): diferentemente dos *white hats*, os *black hats* utilizam as vulnerabilidades que encontram para obter dados sigilosos, como dados pessoais, senhas, dados bancários etc. São definidos ainda como subcategoria dos *crackers*; c) *Gray Hat*: ao encontrar uma vulnerabilidade no sistema de uma empresa, o *gray hat* observa os dados ali inseridos, por vezes até os divulga, sem cometer crime. Contudo, não informa a empresa sobre a existência da vulnerabilidade. São um “meio termo”, pois não cometem crimes, como os *white hats*, mas não repassam a existência de vulnerabilidade à empresa, como os *black hats*; d) *Script Kiddies*: não tem um alvo certo. Normalmente, utilizam ferramentas prontas que foram produzidas por algum “*black hat*”, sem saber exatamente como ela funciona. O “*script kid*” é um “experimentador”, e, por este motivo, quando consegue invadir um *site* importante, acaba fazendo um alvoroço e obtendo fama; e) *Hacktivistas*: possuem motivos ideológicos. Tem como objetivo a divulgação de informações esquecidas pelas mídias, atingindo, desta forma, instituições que se encontram em desacordo com o interesse público; f) *Cracker*: possui muito conhecimento informático, tendo como foco principal o funcionamento dos *softwares*. São responsáveis pela criação dos *cracks*, que são ferramentas utilizadas na quebra da ativação de um *software* comercial, facilitando a pirataria. São definidos como criminosos, pois operam em fraudes bancárias e eletrônicas, furto de dados, golpes, entre outros; g) *Phreaker*: especialista em telefonia (móvel ou fixa). Utilizam o serviço de telefonia gratuitamente por meio de programas e equipamentos; h) *Carder*: especialista em fraude de cartão de crédito. Obtém listas de cartões válidos em *sites* de compras, gerando dados falsos que passam pela verificação da autenticidade de um cartão, e clonam cartões válidos/verdadeiros; i) *State Sponsored Hackers* (hackers patrocinados pelo Estado): hackers contratados pelo governo afim de executarem ataques contra outros países, bem como para defender o seu próprio; j) *Spy Hacker*: hackers contratados por empresas para obterem dados sigilosos de empresas

concorrentes; k) *Spammers*: enviam *e-mails* indesejados em massa com propagandas de lojas, revistas para assinatura, produtos em geral, etc.^{XIII}

Interessa nesse artigo os *hackers* considerados criminosos com ações danosas ao erário ou à reputação de instituições culturais. Atividades seguidas e investigadas por distintas agências internacionais que produzem relatórios regulares sobre suas atuações para alertar potenciais vítimas.

Os procedimentos de invasão de sistemas e redes digitais (*hack*) buscam influenciar determinados públicos realizando uma liberação pública ou ameaçando o vazamento de dados importantes^{XIV} caso não lhes sejam atendidas certas reivindicações. São usados ainda para constranger e promover o descrédito daquela instituição.

Tyler Cohen Wood, consultor de segurança cibernética e ex-vice-chefe cibernético da Agência de Inteligência de Defesa, ao afirmar que “não sabia como mais museus ainda não haviam sido atacados por *hackers*”^{XV}, demonstrou ambiguidade entre o assombro e a obviedade da situação, uma vez que museus de arte possuem doadores milionários e bilionários e os dados destes mecenas, bem como as valiosas obras de arte em exposição nas instituições culturais tornam-se chamarizes para extorsões e planos de assaltos físicos aos museus.

O Escritório das Nações Unidas que cuida de Drogas e Crime (UNODC) dedicou seu capítulo 10 do Relatório apresentado em 2010, em Viena, ao Cibercrime. Por “cibercrime” se compreendeu uma ampla variedade de ofensas, incluindo aquelas contra dados e sistemas de computador (“*hackers*”), falsificação e fraude relacionadas a computadores (“*phishing*”), ofensas de conteúdo (disseminação de pornografia infantil) e ofensas de direitos autorais (divulgação de conteúdo pirateado). Ressaltou que a crescente importância da *Internet* e a dependência coletiva dela se tornou responsável por várias novas oportunidades criminais, considerando problemática a fraude bem estabelecida de roubo de identidade.^{XVI}

Dentre as técnicas mais usadas para extração de informações de identidade por métodos relacionados à *Internet* são divididas em três grandes títulos: “*phishing*” ou enganar os usuários da *Internet* a divulgar suas informações pessoais; “*Malware*” ou o uso de *software* instalado não intencionalmente, que coleta e transmite informações pessoais; e “*hacking*”, ou acesso ilegal a sistemas de computador remotamente.^{XVII}

No Brasil, temos vários museus de Arte que movimentam quantias exorbitantes considerando as obras em sua guarda em exposições de longa e curta duração, além das doações de patronos. Um exemplo disso são os Museu de Arte de São Paulo (MASP) e a Pinacoteca do Estado de São Paulo; os Museus de Arte Moderna (MAM) em São Paulo e no Rio de Janeiro; dentre outras instituições na cartografia nacional. Ressaltando-se ainda que parte destas organizações possuem capital e gestão mistas (público-privadas).

Cada vez mais, diante de um mundo altamente digitalizado, principalmente no contexto da Pandemia Mundial da Covid19, quando várias instituições ampliaram o acesso virtual às suas exposições durante o isolamento social (exposição sobre o Egito no Centro Cultural Banco do Brasil (CCBB) no Rio de Janeiro e em São Paulo e do Museu de Antropologia Theo Brandão, em Maceió, pertencente à Universidade Federal de Alagoas – UFAL, com recentes plataformas para visita virtual), o estudo e desenvolvimento de projetos de cibersegurança para museus e centros culturais, tanto nas questões providas pelo segmento da tecnologia da informação (TI), quanto da Engenharia Social, que envolve comportamentos sociais da equipe interna de profissionais das instituições e seus usuários, torna-se premissa fundamental para uma gestão cultural segura e confiável e a expansão das Humanidades Digitais.

Sob esse aspecto, algumas indagações são muito importantes para tratar da cibersegurança frente a *Open Source Intelligence* (OSINT), quando lidamos com o Código Aberto em uma instituição: Como a instituição usa a *internet*? Como a instituição usa a mídia

MELLO, J. C.

social? A instituição possui políticas de segurança/controle de quem e do que as pessoas podem colocar na *internet*? A instituição lida com pagamentos realizados via servidores digitais internos? A instituição emite pagamentos via servidores digitais internos? A instituição usa *call centers*? Onde estão localizadas as centrais digitais, servidores internos (*data centers*), *call centers* e outras bases tecnológicas? A instituição permite que seus profissionais tragam seus próprios dispositivos e o manuseiem em horário de trabalho usando sua rede *Wi-fi*? A instituição é local ou possui sucursais? O organograma institucional está disponível?^{xviii}

Cabe ainda questionar se a instituição usa os serviços de armazenamento em nuvem (*cloud*)? E como tem lidado com Coletivos de Arte que usam a tecnologia para “invasões artísticas”, usando a realidade aumentada para interferir virtualmente na estética física de exposições?

“Hello, we're from the internet”: Do MoMAR (New York) ao Recycle Group (Paris)

Em 2011, no bojo da Primavera Árabe, o movimento social denominado “*Occupy Wall Street*” (2011) foi desencadeado pelo colapso de um modelo de crescimento econômico estadunidense pautado pelo consumo/endividamento (crise dos *subprimes* de 2007) que a partir da especulação bancária que asfixiou a economia gerando falências, desemprego, confisco de hipotecas de moradias, entre outros impactos na vida da população.^{xix}

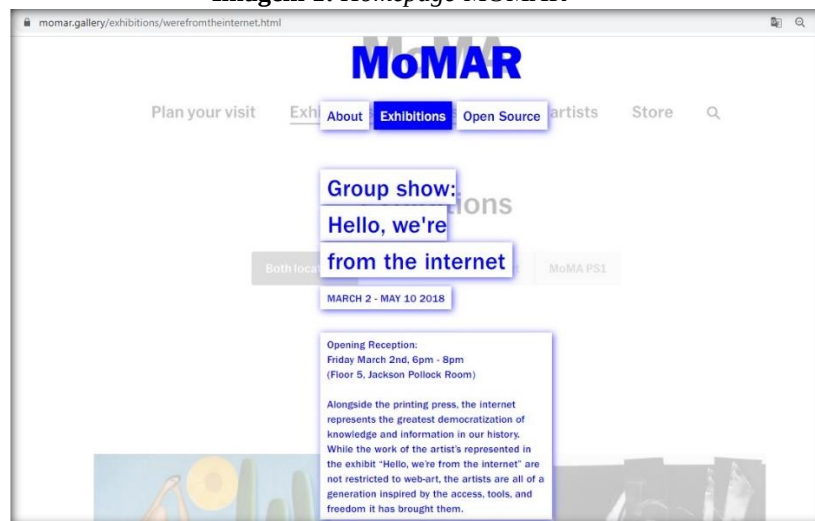
O *Occupy Museum*, em 2012, nasceu como um movimento artístico de protesto contra galerias e museus em Nova Iorque que restringem a montagem de exposições de artistas plásticos sem influência política ou socioeconômica. Desempregados, vagam entre a miséria e o anonimato, não conseguindo nem mesmo uma ocupação no ensino de Artes, uma vez que esse mercado absorvia somente os formados em Escolas de Artes privadas, com indicação.^{xx}

A formação de coletivos de protesto nas artes não é uma novidade, pois o *Guerrilla Girls*, em Nova York desde 1985, enquanto um grupo de artistas feministas anônimas atua intensamente até hoje no combate ao sexismo e o machismo no mundo da arte. Sua missão tem sido expor ao público a desigualdade de gênero e raça dentro da comunidade artística, questionando o quantitativo insignificante de artistas mulheres com trabalhos em exposições de grandes museus e galerias, principalmente quando estas são negras.^{xxi}

Todavia, o *Occupy Museum* destacou-se em 2012 pelo uso de recursos tecnológicos digitais de protesto, como a projeção de imagens nas paredes dos museus contestados. Até então, as manifestações eram analógicas. Era uma questão de tempo para que outros coletivos de arte se apropriassem de ferramentas digitais mais sofisticadas para dar visibilidade às suas demandas contemporâneas.

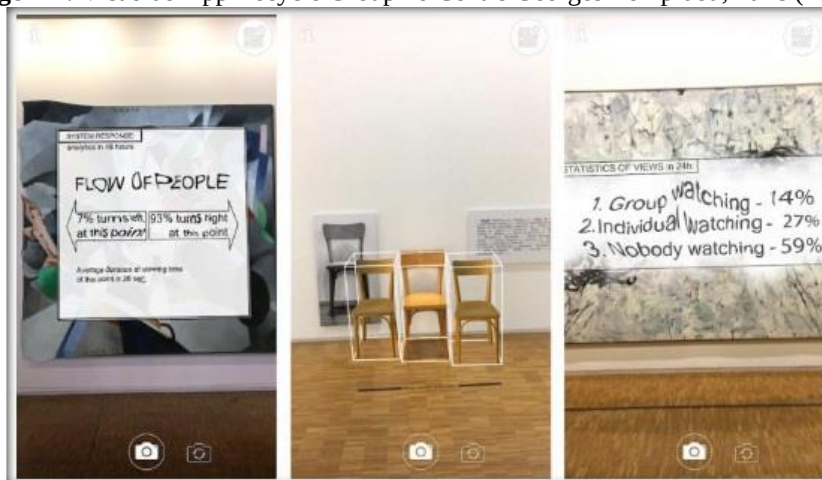
Entre março de 2018, o coletivo Museu de Realidade Aumentada do Museu de Arte Moderna (MoMAR), formado por oito artistas, utilizou a Realidade Aumentada (RA), para “invadir” a sala Jackson Pollock no Museu de Arte Moderna de Nova York (MOMA). Visitantes do museu baixaram um aplicativo da Galeria MoMAR em seus *smartphones* que permitia visualizar intervenções virtuais quando as câmeras eram direcionadas as obras expostas no ambiente físico. Com imagens que se sobrepunham às originais e contendo um manifesto com o título “*Hello, we're from the internet*” contra o elitismo e a exclusividade na cena artística nova-iorquina, os dispositivos móveis dos visitantes possibilitaram um *hacking* diferenciado no ambiente físico do museu. Obviamente, a “interação” não foi elaborada ou autorizada pelo MOMA.^{xxii}

MELLO, J. C.

Imagem 1: Homepage MOMAR**Fonte:** Print da homepage do Momar Gallery Disponível em:<https://momar.gallery/exhibitions/werefromtheinternet.html>, acesso em: 04 jun. 2020.

Artistas visuais como Gabriel Barcia-Colombo interferiram virtualmente na pintura *White Light* (1956) de Jackson Pollock. Articulando sua expertise em memorização e vida pós-morte a obra de Pollock foi reinterpretada. Se o físico continuava inalterado, sob as lentes de um *smartphone* a pintura ganhou novas interações. A inovadora exposição do MoMAR ainda incluiu outras obras que não dialogavam com a sala de Pollock, eram invasões que se apossavam do museu. O coletivo MoMAR tem como missão imiscuir arte virtual na estática das exposições museais, evidenciando sua defasagem criativa na realização de um novo modelo de crítica institucional.^{XXIII}

Em maio de 2018 foi o Centro Cultural Georges-Pompidou, em Paris, hackeado da mesma forma pelo App do Recycle Group sob o lema “*They’re Were Lying To You, Everything Is Different*”.

Imagem 2: Visão do App Recycle Group no Centre Georges-Pompidou, Paris (2018)

Fonte: MAFFEI, 2018. Disponível em: http://www.observatoire-art-contemporain.com/revue_decryptage/tendance_a_suivre.php?langue=en&id=20120955, acesso em: 04 jun. 2020.

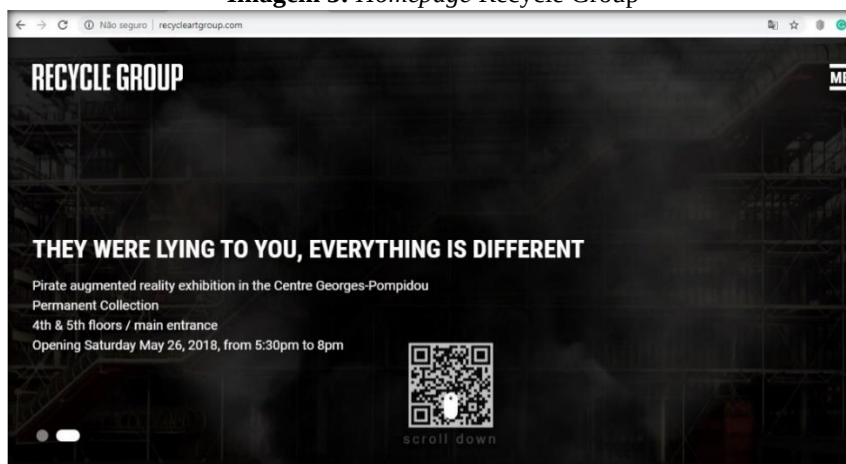
No Centro Cultural Georges Pompidou, o coletivo Recycle Group inseriu mais duas cadeiras virtuais, deixando a cadeira de Joseph Kosuth (*One and Three Chairs*, 1965); além de

MELLO, J. C.

expor um quadro com o percentual de visualização da pintura *Bildübereins* (1991) de Georg Baselitz nas últimas vinte e quatro horas. Outras obras refletiam os objetos por trás do visitante. Algumas pinturas se transformaram em janelas, ignorando as obras de arte para mostrar ao visitante o espaço atrás da parede. No caso de *L'Aubade* de Picasso, o aplicativo deixou à vista a sala ao lado, à noite, com as luzes apagadas, trazendo o cenário de uma hora do dia em que a instituição estava fechada ao público.^{XXIV}

Essas intervenções, ainda que virtuais, colocam em evidência a discussão necessária sobre direitos de propriedade intelectual, ou seja, os direitos autorais das obras expostas, um tema do qual os museus sob ataques dos coletivos artísticos de protesto não podem se furtar. Embora nos dois casos, do MOMA e do Centre Pompidou, a opção tenha sido pelo silêncio quanto à ação realizada, abrindo margem para replicação em outros museus mundo afora.

Imagem 3: Homepage Recycle Group



Fonte: Print de: <http://recycleartgroup.com/>, acesso em: 05/06/2020

A homepage do Recycle Group instrui como utilizar a Realidade Aumentada pirata no Centro Georges-Pompidou explorando a relação entre inteligência artificial e realidade tangível. Através da tecnologia digital o Recycle Group propõe o questionamento do valor cultural, social e político da arte do museu.

O Escritório das Nações Unidas sobre Drogas e Crime (UNODC), uma agência especializada criada pela ONU em 1997, tem alertado em seus relatórios para a ocorrência contínua de violações de propriedade intelectual, pois mais acesso à tecnologia favoreceu o crime cibernético. Ferramentas de *software* adquiridas *on-line* permitem ao usuário localizar portas abertas ou superar a proteção por senha. Essas ferramentas tornam um número muito maior de pessoas em ofensores, não apenas aquelas com habilidades específicas para a computação.^{XXV}

Diante dessa situação, cabe refletir sobre a relação entre os curadores e artistas plásticos em exposição com essas instituições, bem como a relação dos financiadores (doadores) e proprietários de obras que às mantêm sob empréstimo e permutas (comutado) nas coleções de grandes instituições com a omissão das instituições. Seria uma “permissividade”? Interessaria manter as boas tratativas após um ataque deste que gerou visibilidade à instituição?

“I See You, I hack You!” Crimes Cibernéticos em quatro grandes museus de Londres (UK)

O portal *Evening Standard*, em sua matéria de 15 de março de 2019, informou que quatro instituições de Londres, o Museu de História Natural, o Imperial War Museum, o Kew

MELLO, J. C.

Gardens e o Tate identificaram dezenas de milhões de ataques cibernéticos nos últimos anos. Os *hackers* estavam interessados nos dados financeiros pessoais das organizações.

O “*phishing*” ou “fraude de identidade” busca enganar as vítimas na divulgação de senhas e informações relacionadas, fazendo-se passar por instituição financeira relevante ou outra organização com interesse legítimo nessas informações. Ocorre através de *e-mail* e “*pharming*”. O Grupo de Trabalho Anti-*Phishing* identificou 259 campanhas de informações por e-mail que haviam sido sequestradas por *phishers* em junho de 2009. Os setores mais direcionados foram os serviços de pagamento (49%) e o setor financeiro (32%).^{XXVI}

Dados do Parliament Street Institut revelam os quantitativos e tipologias dos ataques dessas instituições:

Quadro 1: Ciber Crimes nos museus de Londres (2016-2018)

Organizações	Tipologia de ciber crimes	Quantitativo
Kew Gardens	<i>Spyware</i>	13,1 milhões (2016-2017) +82,1 milhões (2017-2018)
Imperial War Museum	Não informado	10 milhões (2016-2018)
Tate	<i>Malware/ E-mail de spam</i>	494.709
Museu de História Natural	Não informado	Não informado

Fonte: DAVENPORT, 2019

Especialistas em TI, como Tim Dunton da empresa TI Nimbus Hosting, salientaram os esforços feitos pelos *hackers* para obter informações confidenciais resultando em um alto número de ataques. Charlie McMurdie, ex-líder da equipe de ciber crimes do MET, apontou o uso de “*bots*” automatizados em milhões de ataques, com quadrilhas que trocam dados de seus crimes.^{XXVII}

Uma certeza recai sobre todas as organizações: nenhuma está imune aos ciberataques. Deve-se, portanto, adotar melhores práticas de segurança no consumo das informações, para tentar prevenir, defender ou, no limite, responder com rapidez e eficiência, evitando grandes danos aos usuários e à imagem das instituições.

Muitas vezes as instituições optam por não relatar que foram vítimas de ciberataques e isso as coloca em situação de constrangimento público quando a imprensa ou mesmo as redes sociais descobrem e divulgam amplamente. Assim, o incidente deveria ter sido comunicado ao público mais amplo (usuários, parceiros, financiadores), mantendo o controle das informações e a visibilidade sobre as ações de gerenciamento de crise (Preparação, Detecção e Análise, Contenção, Erradicação e Recuperação, Pós *Mortem*) para garantir que a reputação da organização cultural não seja mais afetada, além de assegurar a confiança dos colaboradores e usuários nas políticas de transparência e resolução de problemas institucionais.

Hackeando o Rijksmuseum Twenthe (Holanda)

Em abril de 2020 os jornais *The Telegraph*^{XXVIII} e *The Sunday Times*^{XXIX}, anunciaram que hackers, fingindo ser comerciantes de arte, convenceram o Rijksmuseum Twenthe, na Holanda, a pagar-lhes £ 2,4 milhões pela pintura *A View of Hampstead Heath: Child's Hill, Harrow in the Distance* (1824) de John Constable. Os criminosos interceptaram *e-mails* entre o Rijksmuseum Twenthe e Simon Dickinson Ltd., um negociante de arte de Londres, que estava organizando a venda da obra de arte. Passando-se por Dickinson instruíram o museu a depositar o valor acordado em uma conta bancária com sede em Hong Kong.

MELLO, J. C.

A notícia explodiu como uma bomba no mundo dos museus de arte e na verdade, chegou atrasada aos jornais, uma vez que desde janeiro de 2020, a Bloomberg^{xxx} já havia anunciado a fraude contra museu e casa negociadora de arte. Entretanto, somente quando o caso tomou uma dimensão judicial a publicização ocorreu. A ausência de uma gestão de cibersegurança eficiente novamente assumia o protagonismo no mundo dos museus de arte.

Ambos entraram em litígio judicial pela posse da obra de arte em questão, porém, o Tribunal de Londres rejeitou as alegações iniciais do museu que inferiu negligência à Dickinson Ltd. Emma Ward, diretora administrativa de Dickinson, chamou atenção para “os perigos do crime cibernético no mundo da arte” vitimando museu e negociador nesse episódio.^{xxxi}

A Engenharia Social se tornou um dos vetores de ataque mais prevalentes e um dos mais difíceis de se defender, pois envolve o comportamento humano em suas fragilidades. Muitos ataques sofisticados e combinados incorporam invariavelmente alguma forma de Engenharia Social. Identificaram-se os ataques direcionados de *spearphishing* como uma tendência crescente em 2014 e dois terços dos incidentes de ciberespionagem apresentaram *phishing*.^{xxxii}

No caso específico do Rijksmuseum Twenthe houve um cibercrime usando *spearphishing*, ou seja, um contato sofisticado com as vítimas hackeadas, via um endereço de *e-mail* bem elaborado ou o endereço real do negociador que o usuário conhecia e teve a conta invadida, para indicar a conta bancária para onde deveria seguir a transferência financeira.

Por isso, é necessário dedicar-se à conscientização das pessoas tanto na prevenção quanto durante a gestão de uma crise gerada por um cibercrime. Esse processo deve ocorrer de forma contínua, através da educação/formação dos canais internos, colaborativos e externos, promovendo o engajamento de todos nas medidas de segurança digital comportamental, viabilizadas por treinamentos, exercícios e simulações, além da elaboração de manuais, vídeos e outros informativos que auxiliem nesse processo pedagógico. Abre-se, portanto, um novo nicho de oportunidades profissionais para graduados nas Humanidades, cujas habilidades didáticas compreendem sua formação. Sob esse aspecto, as formas de expressão e linguagem das humanidades se tornam mais inteligíveis ao público mais amplo que tende a sentir mais dificuldade aos norteamentos dados pelas equipes de TI.

Museum Ciberhacking: mapeando riscos digitais e humanos

A Museologia, em histórico de renovação e aproximação com as comunidades, tornando o museu um espaço de interação do usuário com o conhecimento comunicado, mediado por profissionais cada vez mais imersos no mundo das digitalizações, tanto sofre quanto produz interferências na dinâmica informacional da sociedade. Sua aproximação com a Ciência da Informação, Biblioteconomia e Arquivologia busca a compreensão da organização da cultura que é produzida, reproduzida e transformada pelas instituições que abrigam seu ofício. Portanto, fazem parte desse movimento a análise da dinâmica das múltiplas interferências, realizadas por atores institucionais ou não, em diferentes processos de criação, seleção, circulação e apropriação dos registros de conhecimento.^{xxxiii}

Conhecimentos plurais institucionalizados e transformados em *Big Data*, que condicionam memórias, identidades, registros históricos da humanidade em sua existência social, política, econômica e cultural. Dados fluidos no universo digital e que por isso podem ser invadidos, manipulados ou sequestrados.

A cibersegurança da informação busca proteger os dados bem como dos ativos organizacionais das inúmeras ameaças do mundo virtual. Isto posto que a cadeia de proteção informacional abrange a confidencialidade (evitando acessos não autorizados, perdas, danos ou

MELLO, J. C.

uso inapropriado), integridade (evitar mudanças não solicitadas, garantindo dados exatos e completos) e disponibilidade (concessão de acesso seguro para pessoas certificadas visualizá-las, usá-las e processá-las). Todos esses elementos necessitam de igual atenção e proteção.^{XXXIV}

Por isso planejamento, execução, monitoramento e efetivação de medidas de segurança em contínua atualização e aperfeiçoamento constituem o Ciclo PDCA (*Plan, Do, Check, Act*)^{XXXV}, adotando políticas, normativas e procedimentos em consonância com a legislação, boas práticas de proteção organizacional, ferramentas e tecnologias de controle. Sendo importante também métricas e indicadores que possibilitem identificar tanto o sentido do fluxo da informação, quanto o seu processamento.^{XXXVI}

Para a adoção desses princípios é necessário o desenvolvimento de um novo *framework* institucional, que para além dos procedimentos de segurança digital da equipe de TI, enfatize ainda o treinamento, a capacitação tanto para especialistas, profissionais de instituições culturais, bem como de seus usuários. As pessoas responsáveis pela alimentação cotidiana de plataformas digitais de museus com a agenda de funcionamento (*homepages* e *Apps*), pela catalogação, classificação e documentação do acervo em bancos de dados, pelo *design* criativo das expovirtuais, pela mediação do virtual com o plano físico através das ações educativas na Gameificação (jogos culturais interativos) presente em *homepages*, produção e manutenção das redes sociais de museus (*Facebook, Twitter, Instagram, Whatsapp, Telegram*, etc.), bem como envio e recepção de *e-mails* institucionais precisam ser envolvidas em um programa de segurança da informação, de cibersegurança, centrado nas habilidades e fragilidades humanas.

Tudo o que representa “valor” em uma organização é chamado de “ativo”, portanto, os passos fundamentais para a adoção de um novo *framework* nos museus abrangem: identificar seus ativos e os ricos físicos e virtuais que permeiam a segurança destes.

Imagem 4: Diagrama dos ativos de organizações



Fonte: THOMÉ, 2020, p.3.

A identificação dos processos críticos, “janelas de vulnerabilidade” tecnológicas (*softwares* obsoletos, antivírus gratuitos sem cobertura completa, *data centers* sem proteção, etc.) e humanas (comportamentos danosos como clicar em *e-mails* ou *sites* suspeitos), deve considerar as pessoas importantes (parceiros, funcionários, fornecedores), a documentação de toda a situação (desde as metodologias de prevenção, ao processo de invasão, identificação da origem e procedimentos de resposta e recuperação de dados) para auxiliar e agilizar o trabalho da equipe jurídica (tanto na auditoria interna, quanto na assessoria de comunicação ao público

e processos contra os infratores). Deve ainda envolver o mapeamento dos cenários de crise (de modo preventivo para treinamento e exercício simulado nos momentos de decisão).

Quadro 2: Mapeamento de Riscos Digitais

Ciberataques recorrentes – Definições e práticas
Phishing: infratores desenvolvem <i>sites</i> de empresas que parecem legítimos, conhecidos como “ <i>sites de falsificação</i> ” (<i>spoofy sites</i>), enviando <i>e-mails</i> para atrair suas vítimas. ^{XXXVII}
Pharming: manipulação do DNS (Servidor de Nomes de Domínio) para direcionar o usuário ao falso <i>site</i> , envolvendo a instalação de <i>malware</i> no computador do usuário individual ou em um DNS, que roteia o tráfego na <i>Internet</i> . Com seu computador ou DNS infectado, o usuário que acessa suas contas bancárias eletrônicas ou outras informações <i>online</i> é redirecionado para um <i>site</i> falso. Ao inserir suas informações pessoais para fazer <i>login</i> , os ladrões de identidade registram os dados. ^{XXXVIII}
Malwares: são usados por ladrões de identidade que usam <i>softwares</i> mal-intencionados para obter as informações diretamente do computador do usuário. Podem escanear discos rígidos para coletar informações formatadas de maneira típica de senhas, números de cartão de crédito e números de previdência social. Como muitas pessoas usam as mesmas senhas para várias contas, detectar uma ou duas pode ser suficiente para desbloquear todas as contas dos usuários. ^{XXXIX}
Ransomware: <i>software</i> nocivo que restringe o acesso ao sistema infectado com uma espécie de bloqueio e cobra um resgate em criptomoedas para que o acesso possa ser restabelecido. Caso não ocorra o mesmo, arquivos podem ser deletados ou expostos. ^{XL}
Dyre e Dridex: <i>trojans</i> (<i>malwares</i>) para roubo em transações financeiras. Aparecem na <i>top list</i> dos cibercrimes em diversas organizações. ^{XLI}

Fonte: Elaboração própria a partir de dados coletados.

Observa-se que o universo do ciberhacking é constituído tanto por ameaças às fragilidades gerais humanas e digitais das instituições, quanto de procedimentos para reconhecimento da crise e rapidez na ação de contenção e retomada de controle.

Outubro de 2016, no Reino Unido, foi dedicado à informação e conscientização sobre a segurança cibernética, tendo em vista ser um mês com menos ataques: apenas 140 milhões (!). Sob esse aspecto, pesquisadores do Museu Victoria, na Austrália, recomendaram a aplicação de criptografia incluindo cartões ATM, senhas de computador, comércio eletrônico, gerenciamento de direitos digitais e direitos autorais também para museus, além de um permanente esforço de informação e formação da equipe que trabalha nas instituições.^{XLII} Pois, reafirmava-se que:

Uma compreensão das ameaças cibernéticas potenciais é fundamental para desenvolver estratégias de prevenção aplicadas em toda a infraestrutura de TIC. Cada membro da equipe tem um papel a desempenhar na proteção da confidencialidade, integridade e disponibilidade dos dados de seu museu.^{XLIII}

Em 2020, pesquisas sobre a vulnerabilidade dos Museus Virtuais na Rússia revelaram que a maior parte dos ataques nas plataformas digitais das instituições acontece no recurso SQL (*Structured Query Language*). Conforme os dados da Akamai Intelligent Edge Platform, isso ocorre porque o SQL é a linguagem de programação mais comumente usada na criação de sistemas gerais de bancos de dados (SGBD). Somente no dia 06 de setembro de 2020 foram detectados mais de 71.717.000 ataques a recursos da web (Quadro 3).^{XLIV}.

Quadro 3: Ataques às plataformas digitais em setembro de 2020

Linguagem de Programação	Quantitativo de Ataques	Porcentagem
Recurso SQL	64.851.530	90,43%
Cross-Site Scripting	3.719.830	5,19%
Inclusão de arquivo remoto	3.107.860	4,33%
Recurso PHP	24.820	0,03%
Ferramentas de comando	12.960	0,02%

Fonte: MITYUSHIN, 2021, p.4.

A premissa mais verdadeira em uma organização que precisa lidar com a cibersegurança está no fato de que embora se empreendam esforços tecnológicos e recursos financeiros para proteger as redes e sistemas, o elo mais fraco da segurança ainda é o fator humano. Isto porque sejam instituições totalmente digitais (como o Museu da Pessoa) ou híbridas (como o Museu da Língua Portuguesa, o Museu do Futebol, Museu da Gente Sergipana ou o Itaú Cultural) no que diz respeito ao armazenamento em *data centers* de modo físico na própria instituição ou aliando esse processo à migração em nuvem (*cloud*), o cliente (gestor/instituição) será sempre responsável pela proteção da informação mesmo com a adoção da responsabilidade compartilhada padrão do mercado oferecida por empresas como Google, Amazon Web Service, Microsoft ou outras.

Novas leis de privacidade e gerenciamento de crises cibernéticas têm sido criadas e regulamentadas para garantir a clareza no consentimento do usuário (titular da informação) sobre seus dados e o bom gerenciamento de incidentes no viés das auditorias e respostas jurídicas (processos, indenizações, multas). Já são mais de 120 territórios a adotar tais preocupações frente esse movimento de transformação digital exponencial. Na Europa, a EU General Data Protection Regulation (GDPR) está em vigor desde 25 de maio de 2018 e uma das principais obrigatoriedades é o cumprimento de até 72h para a comunicação aos usuários de ciberataques em seus sistemas. No Brasil, em 2018, foi criada a Lei Geral de Proteção de Dados (LGPD) nº13.709, que ainda está em processo de regulamentação e não tem clareza sobre o “prazo razoável” (se propôs de 5 a 10 dias) para a notificação de incidentes de segurança digital.^{XLV}

Considerações Finais

A contemporaneidade com sua rápida transformação digital em várias partes do mundo e alcançando até mesmo aqueles com menor desenvolvimento tecnológico têm exigido das instituições culturais, museus e centros culturais, adaptação ao contexto da digitalização de dados e acervos. O processo de migração para nuvens de informações e expografias envolve a preocupação com a “segurança *by design*”, ou seja, o planejamento da segurança desde o início.

Nos últimos anos, inúmeros museus e centros culturais internacionais foram alvo de cibercrimes, causando ranhuras em sua imagem pública institucional. O sequestro de *homepages* e dados, a alteração de informações às vésperas da inauguração de uma exposição, os milhões de *malwares*, *spywares* e mesmo *ransomwares* com sequestro do sistema operacional, exigência de resgate em criptomoedas ou a interferência em negociações de compra e venda de obras de arte demonstra que nenhuma organização é infalível.

Os espaços de salvaguarda cultural são também alvos de *hackers* e mais do que uma equipe de TI preparada para atuar na proteção digital, é necessário um diálogo da equipe do museu – composta por muitos profissionais das humanidades – na observação dos comportamentos sociais (Engenharia Social) para através de treinamento com informação/formação e assunção de responsabilidade compartilhada.

Com a legislação aprovada no país (LGPD), as instituições terão que estar cada vez mais atentas aos incidentes digitais que colocam em risco os dados de seus usuários, parceiros e financiadores, sendo transparentes na comunicação do ocorrido, bem como na rapidez da resposta de identificação, contenção e recuperação.

Também as relações entre direitos autorais e intervenções de coletivos artísticos que usam de aplicativos virtuais para invasão das obras de arte físicas são novas situações que precisam ser deliberadas pelas instituições para que seu relacionamento com investidores, curadores e artistas de suas exposições não seja inviabilizado.

Museólogos, historiadores, arqueólogos, antropólogos, pedagogos e demais profissionais da equipe de um museu necessitam conhecer as ameaças à segurança de sua instituição, comprometendo-se a evitar que sejam eles próprios os vetores de invasões em razão de uso descuidado de smartphones pessoais no local do trabalho. Pois muitas vezes o ato mais rudimentar pode fazer eclodir uma crise cibernética sem proporções. Tais profissionais podem e devem se especializar nos treinamentos das equipes, adotando métodos ágeis, colaborativos, criativos e resilientes, oportunizando assim um novo nicho de formação e empregabilidade.

Cientistas da Informação e a equipe jurídica deverão trabalhar em conjunto para que a documentação dos processos de prevenção de ataques, ataques virtuais e procedimentos de respostas auxiliem nas auditorias e eventuais judicializações.

A revolução 4.0 é uma realidade e a transformação digital de museus e centros culturais não está condicionada ao “se”, mas ao “quando”. Estar pronto para decidir em momentos de crise tornará o profissional necessário à instituição e às demandas do tempo presente e futuro.

Notas

^I Doutora em História Social (UFRJ); Professora Adjunta na Universidade Federal de Sergipe (UFS). Membro do GET-UFS.

^{II} ZIEZULEWICZ, G. National Museum of Mexican Art website taken over by hacker. **Chicago Tribune**, 16 abri. 2015. Disponível em: <<https://www.chicagotribune.com/news/ct-mexican-museum-hack-met-20150416-story.html>>. Acesso em: 15 dez. 2019.

^{III} SOUSA, M.C.P. **Humanidades Digitais?** Um breve panorama. (2011). Disponível em: <<https://nehilp.prp.usp.br/~nehilp/HD/SobreHD.html>>. Acesso em: 05 ago. 2020.

^{IV} AUTORIA COLETIVA. **Manifesto das Humanidades Digitais**. THATCamp (2010). Disponível em: <https://humanidadesdigitais.files.wordpress.com/2011/10/poster_manifesto_hd_portugues.pdf>. Acesso em: 05 ago. 2020.

^V SOUSA, M. C. P. **Op. Cit.**

^{VI} UNODC. The globalization of crime. A transnational organized crime threat assessment. **Report 2010**. Vienna: United Nations Publication, 2010, p.204.

^{VII} ARAÚJO, C. A. A. **O que é Ciência da Informação**. Belo Horizonte: KMA, 2018, p.6.

^{VIII} HADNAGY, C. **Social Engineering**. The Science of Human Hacking. 2ª Ed. Toronto: Wiley, 2018, p.55.

^{IX} Idem, ibidem, p.2.

^X CASCONI, S. Hackers Saw the Asian Art Museum of San Francisco as Ripe for a Ransom Attack. Are Other Cultural Institutions Next? **ArtNet News**, 22 jul. 2019. Disponível em: <<https://news.artnet.com/market/hackers-attack-asian-art-museum-san-francisco-1604188>>. Acesso em: 02 abr. 2020.

^{XI} EUROPOL. The Internet Organised Crime Threat Assessment (IOCTA). **Report 2015**. Netherlands: European Police Office, 2015, p.7.

^{XII} E-GOV/UFSC. **Saiba a diferença entre Hackers, Crackers, White Hat, Black Hat, Gray Hat, entre outros**. (2016). Disponível em: <<https://egov.ufsc.br/portal/conteudo/saiba-diferen%C3%A7a-entre-hackers-crackers-white-hat-black-hat-gray-hat-entre-outros>>. Acesso em: 18 set. 2020.

^{XIII} Idem, ibidem.

^{XIV} SHIRES, J. Hack-and-leak operations: intrusion and influence in the Gulf. **Journal of Cyber Policy**. 2019. Disponível em: <<https://doi.org/10.1080/23738871.2019.1636108>>. Acesso em: 02 mai. 2020.

^{XV} CASCONI, S. **Op. Cit.**

^{XVI} UNDOC. **Op. Cit.**, p.203.

-
- xvii Idem, ibidem, p.206.
- xviii HADNAGY, C. **Op. Cit.**, p.58-59.
- xix SAUVIAT, Catherine. Occupy Wall Street, um movimento social inédito nos Estados Unidos. **Cadernos do Desenvolvimento**, vol.7, n°11, pp. 145-159, 2012. Disponível em: <<file:///C:/Users/55799/Downloads/192-653-1-PB.pdf>>. Acesso em: 20 ago. 2020.
- xx OLIVEIRA, Heyse de Souza. HACKEANDO MUSEUS: movimentos de protesto no campo das artes do século 21. **Revista Galo**, Ano 1, n° 2, p.215-223, 2020. Disponível em: <<https://revistagalo.com.br/edi%C3%A7%C3%B5es/edi%C3%A7%C3%A3o-002/18-hackeando-museus/galo-ed2-215-224.pdf?>> Acesso em: 20 jan. 2021.
- xxi NICOLAI, Joe. **GUERRILLA GIRLS**: a igualdade de gênero no universo da arte. (2017). Disponível em: <<https://www.ufrgs.br/arteversa/guerrilla-girls-a-igualdade-de-genero-no-universo-da-arte/>>. Acesso em: 20 jan. 2021.
- xxii VEIGA, A. C. R. Professora da ECI afirma que invasão do digital em ambientes museológicos já é uma realidade. **Arte e Cultura**. 10 mai. 2018. Disponível em: <<https://ufmg.br/comunicacao/noticias/artigo-museus-hiperconectados>>. Acesso em: 04 jun. 2020; PINTO, F. J. S. **Cyborg Art**. Uma Reflexão Sobre o Impacto Das Redes Sociais na Arte Contemporânea. Trabalho de Projeto Mestrado em Arte Multimídia/ Especialização em Audiovisuais. Lisboa: Universidade de Lisboa, 2018, p.40-41.
- xxiii MAFFEI, M. MoMAR: pirating a Museum through augmented reality. **Observatoire de l'art contemporain**, 27 jul. 2018. Disponível em: <http://www.observatoire-art-contemporain.com/revue_decryptage/tendance_a_suivre.php?langue=en&id=20120955>. Acesso em: 04 jun. 2020.
- xxiv Idem, ibidem.
- xxv UNDOC. **Op. Cit.**, p.204.
- xxvi Idem, ibidem, p.206.
- xxvii DAVENPORT, J. Millions of cyber attacks on Kew Gardens and museums as hackers target people's financial data. **Evening Standard**. 15 mar. 2019. Disponível em: <<https://www.standard.co.uk/news/crime/millions-of-cyber-attacks-on-kew-gardens-and-museums-as-hackers-target-people-s-financial-data-a4092871.html>>. Acesso em: 06 jun. 2020.
- xxviii SOUTHWORTH, P. Hackers pretending to be art dealer convinced museum to pay them £2m for John Constable painting. **The Telegraph**, 11 abr. 2020. Disponível em: <<https://www.telegraph.co.uk/news/2020/04/11/hackers-pretending-art-dealer-convinced-museum-pay-2m-john-constable/>>. Acesso em: 06 jun. 2020.
- xxix MALVERN, J. Hackers take £2,4m from Constable Sale. **The Sunday Times**, 13 abr. 2020. Disponível em: <<https://www.thetimes.co.uk/article/hackers-take-2-4m-from-constable-sale-pvktfjqr>>. Acesso em: 06 jun. 2020.
- xxx MILLIGAN, E. Fraudsters Posing as Art Dealer Got Gallery to Pay Millions. **Bloomberg** (Cybersecurity), 30 jan. 2020. Disponível em: <<https://www.bloomberg.com/news/articles/2020-01-30/fraudsters-posing-as-art-dealer-got-gallery-to-transfer-millions>>. Acesso em: 06 jun. 2020.
- xxxi DAFOE, T. A Hacker Posing as a Venerable British Art Dealer Swindled a Dutch Museum Out of \$3.1 Million. **ArtNet News** (Art and Law), 30 jan. 2020. Disponível em: <<https://news.artnet.com/art-world/rijksmuseum-twenthe-simon-dickinson-1765983>>. Acesso em: 06 jun. 2020.
- xxxii EUROPOL. **Op. Cit.**, p. 37.
- xxxiii ARAÚJO, U. Estratégias de comunicação e gestão de crises. **Pós-Graduação em Cibersegurança e Proteção Digital de Negócios**. Vol.1. São Paulo: FIA, 2020, p.71-72.
- xxxiv THOMÉ, A. Conceitos de Segurança da Informação. **Ciberhacking**. Vol.1. São Paulo: FIA, 2020.
- xxxv Idem, ibidem, p.3
- xxxvi Idem, ibid.
- xxxvii UNDOC. **Op. Cit.**, p.207.
- xxxviii Idem, ibidem
- xxxix Idem, ibid.
- xl LISKA, A.; GALLO, T. **Ransomware**: defendendo-se da extorsão digital. São Paulo: Novatec, 2017.
- xli THAKKAR, D. **Preventing Digital Extortion**. Mitigate Ransomware, DDoS and other cyber-extortion attacks. Birmingham/Mumbai: Packt, 2017, p.51.
- xlII PRYOR, W. Staying Safe: Cybersecurity In Modern Museums. **MW17: Museums and the Web 2017**, Cleveland, Ohio, 2017. Disponível em: <<https://mw17.mwconf.org/paper/staying-safe-cybersecurity-in-modern-museums-internal-external-and-hidden-threats-with-a-focus-on-cryptography-to-maintain-data-security/>>. Acesso em: 20 jan. 2021.
- xlIII Idem, ibidem.

^{XLIV} MITYUSHIN, D. A. Information security aspects of virtual museums in Russia. **IOP Conf. Series: Materials Science and Engineering**, Vol. 1047, III International Conference MIST: Aerospace 2020: Advanced Technologies in Aerospace, Mechanical and Automation Engineering (Aerospace 2020) 20st-21nd, November 2020, Krasnoyarsk, Russia. Disponível em: <<https://iopscience.iop.org/article/10.1088/1757-899X/1047/1/012087/meta>>, Acesso em: 18 jul. 2021.

^{XLV} ARAÚJO, U. **Op. Cit.**, p.11-13.

Referências

ARAÚJO, C. A. A. **O que é Ciência da Informação**. Belo Horizonte: KMA, 2018.

ARAÚJO, U. Estratégias de comunicação e gestão de crises. **Pós-Graduação em Cibersegurança e Proteção Digital de Negócios**. Vol.1. São Paulo: FIA, 2020.

AUTORIA COLETIVA. **Manifesto das Humanidades Digitais**. THATCamp (2010). Disponível em: https://humanidadesdigitais.files.wordpress.com/2011/10/poster_manifesto_hd_portugues.pdf. Acesso em: 05 ago. 2020.

CASCONI, S. Hackers Saw the Asian Art Museum of San Francisco as Ripe for a Ransom Attack. Are Other Cultural Institutions Next? **ArtNet News**, 22 jul. 2019. Disponível em: <<https://news.artnet.com/market/hackers-attack-asian-art-museum-san-francisco-1604188>>. Acesso em: 02 abr. 2020.

DAFOE, T. A Hacker Posing as a Venerable British Art Dealer Swindled a Dutch Museum Out of \$3.1 Million. **ArtNet News** (Art and Law), 30 jan. 2020. Disponível em: <<https://news.artnet.com/art-world/rijksmuseum-twenthe-simon-dickinson-1765983>>. Acesso em: 06 jun. 2020.

DAVENPORT, J. Millions of cyber attacks on Kew Gardens and museums as hackers target people's financial data. **Evening Standard**. 15 mar. 2019. Disponível em: <<https://www.standard.co.uk/news/crime/millions-of-cyber-attacks-on-kew-gardens-and-museums-as-hackers-target-people-s-financial-data-a4092871.html>>. Acesso em: 06 jun. 2020.

E-GOV/UFSC. **Saiba a diferença entre Hackers, Crackers, White Hat, Black Hat, Gray Hat, entre outros**. (2016). Disponível em: <<https://egov.ufsc.br/portal/conteudo/saiba-diferen%C3%A7a-entre-hackers-crackers-white-hat-black-hat-gray-hat-entre-outros>>. Acesso em: 18 set. 2020.

EUROPOL. The Internet Organised Crime Threat Assessment (IOCTA). **Report 2015**. Netherlands: European Police Office, 2015.

HADNAGY, C. **Social Engineering**. The Science of Human Hacking. 2ª Ed. Toronto: Wiley, 2018.

LISKA, A.; GALLO, T. **Ransomware**: defendendo-se da extorsão digital. São Paulo: Novatec, 2017.

MAFFEI, M. MoMAR: pirating a Museum through augmented reality. **Observatoire de l'art contemporain**, 27 jul. 2018. Disponível em: <<http://www.observatoire-art->

contemporain.com/revue_decryptage/tendance_a_suivre.php?langue=en&id=20120955>.

Acesso em: 04 jun. 2020.

MALVERN, J. Hackers take £2,4m from Constable Sale. **The Sunday Times**, 13 abr. 2020. Disponível em: <<https://www.thetimes.co.uk/article/hackers-take-2-4m-from-constable-sale-pvktfjqrr>>. Acesso em: 06 jun. 2020.

MILLIGAN, E. Fraudsters Posing as Art Dealer Got Gallery to Pay Millions. **Bloomberg** (Cybersecurity), 30 jan. 2020. Disponível em: <<https://www.bloomberg.com/news/articles/2020-01-30/fraudsters-posing-as-art-dealer-got-gallery-to-transfer-millions>>. Acesso em: 06 jun. 2020.

MITYUSHIN, D. A. Information security aspects of virtual museums in Russia. **IOP Conf. Series: Materials Science and Engineering**, Vol. 1047, III International Conference MIST: Aerospace 2020: Advanced Technologies in Aerospace, Mechanical and Automation Engineering (Aerospace 2020) 20st-21nd, November 2020, Krasnoyarsk, Russia. Disponível em: <https://iopscience.iop.org/article/10.1088/1757-899X/1047/1/012087/meta>, Acesso em: 18 jul. 2021.

NICOLAI, Joe. **GUERRILLA GIRLS**: a igualdade de gênero no universo da arte. (2017). Disponível em: <https://www.ufrgs.br/artevera/guerrilla-girls-a-igualdade-de-genero-no-universo-da-arte/>. Acesso em: 20 jan. 2021.

OLIVEIRA, Heyse de Souza. HACKEANDO MUSEUS: movimentos de protesto no campo das artes do século 21. **Revista Galo**, Ano 1, nº 2, p.215-223, 2020. Disponível em: <https://revistagalo.com.br/edi%C3%A7%C3%B5es/edi%C3%A7%C3%A3o-002/18-hackeando-museus/galo-ed2-215-224.pdf>? Acesso em: 20 jan. 2021.

PINTO, F. J. S. **Cyborg Art**. Uma Reflexão Sobre o Impacto Das Redes Sociais na Arte Contemporânea. Trabalho de Projeto Mestrado em Arte Multimídia/ Especialização em Audiovisuais. Lisboa: Universidade de Lisboa, 2018.

PRYOR, W. Staying Safe: Cybersecurity In Modern Museums. **MW17: Museums and the Web 2017**, Cleveland, Ohio, 2017. Disponível em: <https://mw17.mwconf.org/paper/staying-safe-cybersecurity-in-modern-museums-internal-external-and-hidden-threats-with-a-focus-on-cryptography-to-maintain-data-security/>. Acesso em: 20 jan. 2021.

SAUVIAT, Catherine. *Occupy Wall Street*, um movimento social inédito nos Estados Unidos. **Cadernos do Desenvolvimento**, vol.7, nº11, pp. 145-159, 2012. Disponível em: <file:///C:/Users/55799/Downloads/192-653-1-PB.pdf>. Acesso em: 20 ago. 2020.

SHIRES, J. Hack-and-leak operations: intrusion and influence in the Gulf. **Journal of Cyber Policy**. 2019. Disponível em: <<https://doi.org/10.1080/23738871.2019.1636108>>. Acesso em: 02 mai. 2020.

SOUSA, M.C.P. **Humanidades Digitais?** Um breve panorama. (2011). Disponível em: <<https://nehilp.prp.usp.br/~nehilp/HD/SobreHD.html>>. Acesso em: 05 ago. 2020.

SOUTHWORTH, P. Hackers pretending to be art dealer convinced museum to pay them £2m for John Constable painting. **The Telegraph**, 11 abr. 2020. Disponível em: <<https://www.telegraph.co.uk/news/2020/04/11/hackers-pretending-art-dealer-convinced-museum-pay-2m-john-constable/>>. Acesso em: 06 jun. 2020.

THAKKAR, D. **Preventing Digital Extortion**. Mitigate Ransomware, DDoS and other cyber-extortion attacks. Birmingham/Mumbai: Packt, 2017.

THOMÉ, A. Conceitos de Segurança da Informação. **Ciberhacking**. Vol.1. São Paulo: FIA, 2020.

UNODC. **The globalization of crime**. A transnational organized crime threat assessment (Report 2010). Vienna: United Nations Publication, 2010.

VEIGA, A. C. R. Professora da ECI afirma que invasão do digital em ambientes museológicos já é uma realidade. **Arte e Cultura**. 10 mai. 2018. Disponível em: <<https://ufmg.br/comunicacao/noticias/artigo-museus-hiperconectados>>. Acesso em: 04 jun. 2020.

ZIEZULEWICZ, G. National Museum of Mexican Art website taken over by hacker. **Chicago Tribune**, 16 abri. 2015. Disponível em: <<https://www.chicagotribune.com/news/ct-mexican-museum-hack-met-20150416-story.html>>. Acesso em: 15 dez. 2019.