Ciber Proteção e o Ministério Público: interfaces e prospectivas

Eduardo Wallier Vianna

Pesquisador colaborador pleno na Universidade de Brasília (UnB) e pesquisador associado da Escola Superior de Guerra (ESG). Doutor em Ciência da Informação pela Faculdade de Ciência da Informação (FCI/UnB) – "Modelo de ciber proteção nacional".

Resumo: Percebe-se a importância do domínio do espaço cibernético para a sociedade contemporânea, cabendo a cada Estado-Nação organizar, fortalecer e proteger seu ecossistema digital a fim de exercer plenamente sua soberania, seja preservando direitos individuais, seja implementando políticas e ações em prol da sociedade ou da defesa nacional. Apresenta o conceito de Ciber Proteção como um ecossistema complexo, contemplando atividades nas áreas de segurança da informação digital, defesa cibernética, preservação digital e infraestruturas críticas; bem como elenca os principais atores da segurança e da defesa cibernéticas nacionais. Revisa o arcabouço normativo nacional na busca de orientações atualizadas sobre o contexto abrangente da proteção da informação digital. Em seguida, aborda as iniciativas do Ministério Público do Distrito Federal e Territórios, tais como a atualização do seu planejamento estratégico, a criação de unidades e a instituição de comitês e programas sob a ótica da Ciber Proteção. Entende-se que a promoção da cidadania e da justiça pelo Ministério Público deve estar em constante aperfeiçoamento, especialmente na dimensão cibernética, contemplando o uso seguro dos meios digitais pela sociedade brasileira. Como resultado, detalha possíveis contribuições e questionamentos em prol da maturidade na proteção de dados, gestão de incidentes, capacitação cibernética do cidadão e descarte digital.

Palavras-chave: Espaço cibernético. Ciber proteção. Segurança cibernética. Segurança da informação digital. Proteção cibernética.

Sumário: Introdução. 1 Ciber Proteção: visão holística e sistê-

mica. 1.1 O contexto brasileiro. 1.2 A evolução do normativo nacional. 2 Ciber Proteção e o MPDFT. 3 Contribuições para a consolidação da Ciber Proteção no MP. 3.1 Maturidade na proteção de dados pessoais. 3.2 Gestão de incidentes cibernéticos. 3.3 Literacia digital. 3.4 Preservação e descarte digital. 4 Desdobramentos e conclusões. 4.1 Primeira reflexão. 4.2 Segunda reflexão. Referências.

Submissão: 05/08/2022
Aceite: 03/10/2022

Introdução

Iniciada em meados de 2022, a invasão do território Ucraniano pela Rússia, além de provocar muito sofrimento com perdas de vidas, asseverou a importância do domínio do espaço cibernético para a sociedade contemporânea. Podem-se observar não somente ações cibernéticas contra as infraestruturas críticas e estratégicas dos países envolvidos, mas também incontáveis narrativas contraditórias e tresmalhadas, tanto pela mídia tradicional quanto por canais sociais distribuídos pela rede mundial de computadores.

Essencial para a sobrevivência dos Estados e desenvolvimento da sociedade em plena quarta Revolução Industrial ou do Conhecimento[1], o espaço cibernético engloba a Internet e pode ser entendido como um ambiente virtual criado

[1] Considerada como uma nova era de inovação, em que um conjunto de modernas tecnologias estão integrando os mundos físico, digital e tecnológico, influenciando disciplinas, economias e setores cuja característica espacial-chave é a ligação no meio digital, em rede, entre o local e o global (VIANNA, 2019).

pelo ser humano, imprevisível, propenso a falhas de origem e em constante transformação.

Nesse meio digital, composto basicamente por hardware, software e redes de comunicação, interagem pessoas e organizações, bem como desdobram-se sistemas informacionais que vêm fornecendo uma camada não presencial de relacionamento do cidadão com as diversas estruturas que compõe o Estado-Nação brasileiro. Nesse contexto, a informação digital é considerada como um recurso concreto, tangível, materializado por dígitos binários (zeros e uns) que, na essência, representam a forma física dos objetos informativos disponibilizados.

Ações maliciosas como ataques distribuídos de negação de serviço (DDoS) e sequestro de dados (*ransomware*) podem comprometer o funcionamento desses sistemas digitais, impactando diretamente o exercício da cidadania, a exemplo do que ocorreu em Baltimore (EUA), no ano de 2019. Na ocasião, sistemas do governo local foram infectados com artefatos maliciosos. Bases de dados que suportavam correio eletrônico, movimentações financeiras, cadastros imobiliários, entre outras, foram criptografadas, comprometendo não apenas serviços disponibilizados pela prefeitura, mas todo o sistema digital da cidade. Como medida imediata de contenção de danos, diversos equipamentos foram sumariamente desligados ou desconectados, o que impediu usuários (funcionários e cidadãos) de acessar informações essenciais por semanas, impactando as operações municipais e o cotidiano dos moradores. (ORTIZ, 2019).

Percebe-se a informação digital como um ativo crítico, um recurso individual e coletivo de elevada sensibilidade e relevância que deve ser protegido. Seu comprometimento pode provocar perdas irreversíveis, inviabilizar a continuidade de uma instituição e desestabilizar governos. Nesse sentido, a informação deve ser considerada não somente como um *alvo* de ações maliciosas, mas também como uma *arma* no meio digital, particularmente no ambiente da Ciber Proteção.

O objetivo deste trabalho se concentra em aprofundar a temática da utilização segura do espaço cibernético no âmbito do Ministério Público (MP), em particular a proteção do cidadão na interação com o meio digital. Os objetivos específicos foram: (i) aproximar o conceito da Ciber Proteção ao escopo de atribuições e interesses do MP; (ii) identificar as atividades e iniciativas em desenvolvimento no âmbito do Ministério Público do Distrito Federal e Territórios (MPDFT), sob a perspectiva da Ciber Proteção; e (iii) elencar oportunidades de melhoria para a consolidação da Ciber Proteção no MP.

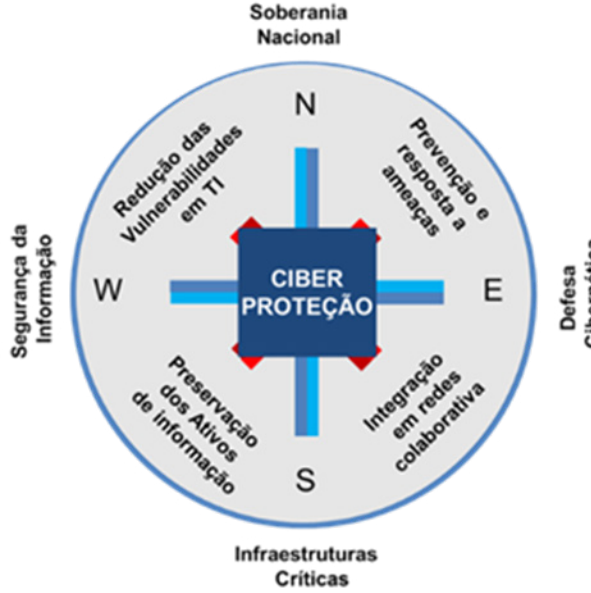
O trabalho justifica-se pelo incremento da utilização do espaço cibernético pela sociedade, pela ampliação dos serviços públicos disponibilizados ao cidadão e o pelo aumento das ações maliciosas no meio digital.

1 Ciber Proteção: visão holística e sistêmica

Neste trabalho, o conceito da Ciber Proteção refere-se à proteção dos sistemas de informação no ciberespaço de interesse nacional.

Seu entendimento demanda adequação à realidade brasileira, possui características típicas da complexidade e da multidisciplinaridade, envolvendo coordenação multissetorial e atividades distintas. A Figura 1 ilustra o conceito da Ciber Proteção, que, em síntese, representa um ecossistema[2] complexo e interdependente.

Figura 1 – Ciber Proteção



Fonte: Elaborado pelo autor (2019).

Ao buscar serviços públicos informatizados, o cidadão e as organizações esperam encontrar sistemas de qualidade, que

[2] Um ecossistema ou macroambiente de Ciber Proteção caracteriza-se pelo emprego, no ciberespaço de interesse nacional ou institucional, de ações típicas de segurança da informação, podendo incluir medidas de defesa cibernética, bem como de preservação digital. Informações adicionais sobre ecossistemas cibernéticos podem ser encontradas em Ishikawa *et al*. (2022).

resolvam tempestivamente suas demandas com objetividade, reduzindo a burocracia.

Esse padrão ideal de interação remete, inexoravelmente, aos pilares da segurança da informação. Em síntese, os dados pessoais ou informações empresariais oriundos das consultas informacionais devem atender a diversos requisitos de segurança, apresentando propriedades e atributos específicos, com destaque para:

a) Confidencialidade (*confidentiality*): propriedade de a informação não ser disponível ou revelada a indivíduos, entidades ou processos não autorizados;

b) Integridade (*integrity*): propriedade de exatidão e completeza;

c) Disponibilidade (*availability*): propriedade de estar acessível e utilizável sob demanda de uma entidade autorizada;

d) Autenticidade (*authenticity*): propriedade de a entidade ser o que diz ser;

e) Responsabilidade (*accountability*): propriedade de o responsável pela informação ter de prestar contas sobre ela;

f) Não repúdio (*non-repudiation*): capacidade de comprovar a ocorrência de reivindicação de um evento ou de uma ação e suas entidades originárias;

g) Confiabilidade (*reliability*): propriedade de o comportamento e o resultado serem consistentes com a intenção (VIANNA, 2019).

1.1 O contexto brasileiro

A segurança da informação é a base da Ciber Proteção e deve ser praticada por toda a sociedade, instituições e organizações. A segurança da informação[3] caracteriza-se por ações sistêmicas e centralizadas, pelo controle da informação disponibilizada em sistemas proprietários e pela busca da conformidade com normas e padrões (por exemplo: família ISO/IEC 27.000). No cenário nacional, destacam-se as seguintes instituições:

a) Gabinete de Segurança Institucional da Presidência da República (GSIPR): orienta a condução de políticas de segurança da informação e comunicações no âmbito da Administração Pública Federal (APF);

b) Departamento de Segurança da Informação (DSI): compõe a estrutura do GSIPR, cooperando no planejamento, coordenação e supervisão da atividade nacional de segurança da informação, incluindo a segurança cibernética, a gestão de incidentes computacionais, a proteção de dados, o credenciamento de segurança e o tratamento de informações sigilosas;

c) Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov): integra o DSI, provendo a APF e sendo responsável por: notificação e análise de incidentes, suporte e

[3] Neste trabalho, considera-se que a segurança da informação deve ser aplicada a qualquer tipo de suporte, seja ele físico ou digital. Assim, quando se trata especificamente de informação digital, é usual utilizar o termo segurança cibernética.

coordenação na resposta a incidentes, distribuição de alertas, recomendações e estatísticas;

d) Comitê Gestor da Internet no Brasil (CGI.br): de acordo com o Decreto nº 4.829, de 3 de setembro de 2003, tem a atribuição de estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, incluindo registro de Nomes de Domínio, alocação de Endereço IP (*Internet Protocol*) e administração do ".br";

e) Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança (CERT.br): integra a estrutura do CGI.br, como grupo responsável por receber, analisar e responder a incidentes de segurança em computadores, envolvendo redes conectadas à Internet brasileira, atuando ainda como ponto de contato nacional para notificação de incidentes de segurança;

f) Centro de Atendimento a Incidentes de Segurança (CAIS): integra a Rede Nacional de Ensino e Pesquisa (RNP), atuando na detecção, resolução e prevenção de incidentes de segurança na rede acadêmica brasileira, além de elaborar, promover e disseminar práticas de segurança em redes de computadores.

A Defesa engloba o conjunto de medidas e ações do Estado, com ênfase no campo militar, para a manutenção do território, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais ou manifestas, atuando em dimensões distintas, como a cibernética. A eficácia das ações de defesa cibernética depende fundamentalmente da atuação

colaborativa da sociedade, incluindo não apenas a expressão militar, mas também a comunidade acadêmica, os setores público e privado e a base industrial de defesa.

No âmbito do Ministério da Defesa, no final do ano de 2020, foi criado o Sistema Militar de Defesa Cibernética (SMDC), entendido como um:

> conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar ações voltadas para assegurar o uso efetivo do espaço cibernético pela Defesa Nacional, bem como impedir ou dificultar ações hostis contra seus interesses. O órgão central do SMDC é o Comando de Defesa Cibernética (ComDCiber), comando operacional conjunto, permanentemente ativado e com capacidade interagências. (BRASIL, 2020b, p. 14).

O ComDCiber – além de um Estado Maior Conjunto e de um Departamento de Gestão Estratégica, que tratam das atividades de planejamento, inteligência, ciência e tecnologia – possui como braço operacional o Centro de Defesa Cibernética (CDCiber), tendo ainda na Escola Nacional de Defesa Cibernética (ENaDCiber) seu vetor de capacitação, pesquisa e inovação.

As infraestruturas críticas (ICs) ou estratégicas para o país também integram o ecossistema da Ciber Proteção e, no Brasil, são entendidas como: "instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade" (BRASIL, 2018a). As ICs estão organizadas em cinco áreas prioritárias:

a) Comunicações: telecomunicações, serviços postais e radiodifusão;

b) Transporte: aquaviário, aéreo e terrestre;

c) Energia: elétrica, petróleo, gás natural e combustível renovável;

d) Água: abastecimento urbano e barragem; e

e) Finanças: bancário e financeiro.

Ataques cibernéticos contra as ICs de um país fazem parte da realidade contemporânea, independentemente de suas motivações (financeira, sabotagem, desestabilização de governos, entre outras), autoria (individual ou grupo constituído), com ou sem patrocínio de um Estado ou grupo adverso (economia concorrente, crime organizado etc.) e formas de realização: ostensivamente (como na guerra entre Rússia e Ucrânia) ou na clandestinidade (o anonimato é o modo mais usual).

A segurança das Infraestruturas Críticas deve ser conduzida de forma matricial, contribuindo para o aumento da capacidade de continuar operando mesmo na presença de falhas ou ações maliciosas (resiliência). A segurança das ICs amalgama diversos atores governamentais (civis e militares) e empresas prestadores de serviços essenciais, sejam públicas ou privadas, incluindo todos os atores envolvidos com a segurança e a defesa cibernéticas anteriormente citados, particularmente o GSIPR e o ComDCiber. A realização anual do *Exercício Guardião Cibernético* materializa, assim, a importância da coordenação interagências ao criar um ambiente realista onde as infraestruturas críticas participantes

precisam proteger seus sistemas de Tecnologia da Informação de ataques cibernéticos[4].

A Soberania, no escopo da Ciber Proteção, relaciona-se notadamente com a segurança e a defesa cibernéticas, consolidando-se por intermédio da projeção do poder cibernético nacional como a capacidade de dissuasão, pela capacidade de resiliência diante de ações adversas e pela resposta ativa a contra ataques às ICs estratégicas.

Não obstante, para a preservação da autoridade e da autonomia do país no cenário internacional, convém destacar a necessidade de uma legislação atualizada com as tendências globais, assim como alinhada com as melhores práticas de proteção do espaço cibernético.

1.2 A evolução do normativo nacional

Os cuidados com a informação digital e, em particular, com o seu uso por meio da Rede Mundial de Computadores foram incrementados, a partir de 2011, com legislação de especial interesse para toda a sociedade brasileira, abordando temas como: acesso à informação, uso da internet, proteção de dados pessoais, transformação digital, crimes cibernéticos e fraudes eletrônicas; com alterações peculiares no Código Penal brasileiro. O Quadro 1 organiza cronologicamente o arcabouço legal, intercalando com

[4] O Exercício Guardião Cibernético, versão 2022, será realizado, simultaneamente, nas cidades de Brasília e São Paulo. Informações complementares sobre a estruturação do Exercício podem ser adquiridas em: https://www.in.gov.br/web/dou/-/edital-de-chamamento-publico-376272001.

outras iniciativas normativas que impactaram, positivamente, o desenvolvimento de um ambiente para a Ciber Proteção nacional.

Quadro 1 – Legislação de interesse para a Ciber Proteção nacional

ANO	LEGISLAÇÃO	EMENTA
2011	Lei nº 12.527, de 18 de novembro	Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal
2012	Lei nº 12.737, de 30 de novembro	Dispõe sobre a tipificação criminal de delitos informáticos (crimes cibernéticos), altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências
2014	Lei nº 12.965, de 23 de abril	Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil e determina as diretrizes para atuação da União, dos estados, do Distrito Federal e dos municípios (Marco Civil da Internet)
2014	Resolução nº 39 CONARQ, de 29 de abril	Estabelece diretrizes para a implementação de repositórios arquivísticos digitais confiáveis (RDC-Arq) para o arquivamento e manutenção de documentos arquivísticos digitais em suas fases corrente, intermediária e permanente
2016	Resolução nº 156 CNMP, de 13 de dezembro	Institui a Política de Segurança Institucional e o Sistema Nacional de Segurança Institucional do Ministério Público, com a finalidade de integrar as ações de planejamento e de execução das atividades de segurança institucional no âmbito do Ministério Público e garantir o pleno exercício das suas atividades

ANO	LEGISLAÇÃO	EMENTA
2017	Resolução nº 171 CNMP, de 27 de junho	Institui a Política Nacional de Tecnologia da Informação do Ministério Público (PNTI-MP), com a finalidade de alinhar as práticas de governança e gestão de TI em todas as unidades e os ramos do Ministério Público
2018	Lei nº 13.709, de 14 de agosto	Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado (Lei Geral de Proteção de Dados Pessoais – LGPD)
2018	Decreto nº 9.573, de 22 de novembro	Aprova a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC), com a finalidade garantir a segurança e a resiliência das infraestruturas críticas do país e a continuidade da prestação de seus serviços
2018	Decreto nº 9.637, de 26 de dezembro	Institui a Política Nacional de Segurança da Informação (PNSI), com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação em âmbito nacional
2019	Resolução nº 11 STJ/GP, de 25 de junho	Institui a Política de Preservação Digital do Superior Tribunal de Justiça, compreende princípios, objetivos, diretrizes e requisitos para a preservação de documentos digitais em Repositório Arquivístico Digital Confiável (RDC-Arq)
2020	Decreto nº 10.222, de 5 de fevereiro	Institui a Estratégia Nacional de Segurança Cibernética (E-Ciber), com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação em âmbito nacional
2020	Decreto nº 10.474, de 26 de agosto	Estrutura e estabelece a Autoridade Nacional de Proteção de Dados (ANPD) em consonância com a LGPD

ANO	LEGISLAÇÃO	EMENTA
2020	Decreto nº 10.569, de 9 dezembro	Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC), que introduz as infraestruturas de comunicações, de energia, de transportes, de finanças e de águas, entre outras, como essenciais para o desenvolvimento econômico sustentável, a integração, a segurança e a soberania do país
2021	Lei nº 14.129, de 29 de março	Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública
2021	Lei nº 14.155, de 27 de maio	Torna mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet
2021	Resolução nº 225 CNMP, de 24 de março	Institui o Plano de Classificação de Documentos do Ministério Público (PCD) e a Tabela de Temporalidade e Destinação de Documentos do Ministério Público (TTD)
2021	Resolução nº 396 CNJ, de 7 de junho	Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), que contempla diversos temas da segurança da informação, como segurança física e proteção de ativos de tecnologia da informação
2021	Decreto nº 10.748 de 16 de julho	Institui a Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC), com a finalidade aprimorar e manter a coordenação entre órgãos e entidades da administração pública federal direta, autárquica e fundacional para prevenção, tratamento e resposta a incidentes cibernéticos

Fonte: Elaborado pelo autor.

Tramita no Congresso Nacional a segunda atualização de documentação inerente à Defesa Nacional, nomeadamente a Política Nacional de Defesa, a Estratégia Nacional de Defesa e o Livro

Branco de Defesa Nacional; ratificando o setor cibernético como um dos três setores tecnológicos essenciais para a Defesa Nacional[5].

Espera-se, também para o ano de 2022, a aprovação do Projeto de Lei (PL) nº 4.401/2021 que dispõe sobre as diretrizes a serem observadas na prestação de serviços de ativos virtuais e na sua regulamentação.

Neste contexto, segundo o Banco Central (BCB, 2020), as *moedas virtuais* são representações digitais de valor, decorrentes da confiança depositada nas suas regras de funcionamento e na cadeia de participantes. Portanto, as mesmas não se confundem com os recursos em reais mantidos em meio eletrônico em bancos e não são emitidas, garantidas ou reguladas pela instituição, reforçando-se que não há legislação ou regulamentação específica sobre o tema no Brasil.

O PL 4.401 propõe que as prestadoras em questão somente poderão funcionar no país mediante prévia autorização de órgão ou de entidade da APF, bem como acresce ao Código Penal artigo que trata da "fraude com a utilização de ativos virtuais, valores mobiliários ou ativos financeiros" (BRASIL, 2021b). O PL também amplia o escopo da proposta inicial de 2015 (focada em moedas virtuais e programas de milhagem), abarcando de forma

[5] Os três documentos devem sofrer atualizações quadrienais pelo Poder Executivo e são encaminhados ao Congresso Nacional para aprovação. Destaca-se a Política Nacional de Defesa, que, voltada prioritariamente para ameaças externas, estabelece objetivos para o preparo e o emprego de todas as expressões do Poder Nacional, em prol da Defesa Nacional. Maiores esclarecimentos estão disponíveis em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congressonacional_22_07_2020.pdf.

mais ampla o tema, possibilitando, por exemplo, a inclusão de regulamentação sobre tokens não fungíveis (NFT), ao definir o termo ativo virtual como:

> a representação digital de valor que pode ser negociada ou transferida por meios eletrônicos e utilizada para a realização de pagamentos ou com o propósito de investimento, não incluídos: I – moeda nacional e moedas estrangeiras; II – moeda eletrônica […]; III – instrumentos que provejam ao seu titular acesso a produtos ou serviços especificados ou a benefício proveniente desses produtos ou serviços, a exemplo de pontos e recompensas de programas de fidelidade; e IV – representações de ativos cuja emissão, escrituração, negociação ou liquidação esteja prevista em lei ou regulamento […]. (BRASIL, 2021b).

O Projeto de Lei 4.401/2021 ainda aponta diretrizes para a prestação de serviço de ativos digitais de especial interesse para as atividades do Ministério Público, tais como: (i) segurança da informação e proteção de dados pessoais; (ii) proteção e defesa de consumidores e usuários; e (iii) prevenção à lavagem de dinheiro e ao financiamento do terrorismo e da proliferação de armas de destruição em massa, em alinhamento com os padrões internacionais.

A seção seguinte aborda algumas iniciativas do Ministério Público do Distrito Federal e Territórios relacionadas de forma direta ou indireta com o discutido neste trabalho sobre Ciber Proteção, tais como: criação de unidades, estabelecimento de programas e iniciativas estratégicas, instituição de políticas/comitês e capacitação de integrantes.

2 Ciber Proteção e o MPDFT

O Planejamento Estratégico Institucional (PEI) para o período 2022 a 2026 do MPDFT assim apresenta a missão da instituição: "Promover a justiça, a democracia, a cidadania e a dignidade humana, atuando para transformar em realidade os direitos da sociedade" (MPDFT, 2022). O PEI utiliza uma cadeia de valor para organizar e agrupar seus três macroprocessos: gestão, governança e finalísticos com o intuito de gerar valor para a organização e para a sociedade.

Por meio de 26 Objetivos Estratégicos (OEs), o MPDFT internaliza tendências e movimentos contemporâneos do espaço cibernético de interesse, onde procura alcançar o crescimento do exercício da cidadania e a consolidação dos direitos da sociedade; bem como enfrentar as vicissitudes que envolvem o uso seguro dos dados e das tecnologias de informação (TI). Buscando aderência holística a temática deste estudo e de forma não exaustiva ou literal, o Quadro 2 relaciona os OEs com algumas ações e iniciativas desdobradas no PEI.

Quadro 2 – Ciber Proteção e o PEI/MPDFT

OE	INICIATIVAS ESTRATÉGICAS
5 Atuação Sustentável	- Executar ações preventivas e informativas sobre a sustentabilidade ambiental, social e econômica
8 Comunicação Institucional	- Padronizar e organizar o acesso aos serviços e informações disponíveis na intranet - Ampliar a participação da instituição nas redes sociais
11 Gestão de Riscos	- Estabelecer contexto para a identificação, análise, avaliação, tratamento, comunicação e monitoramento dos riscos das atividades exercidas pelas unidades e órgãos institucionais
13 Segurança e Inteligência	- Implementar barreiras físicas e virtuais de segurança - Dispor de soluções e inovações tecnológicas que venham robustecer a atividade de segurança e de inteligência - Promover ações voltadas ao desenvolvimento continuado de competências profissionais de segurança e inteligência - Implementar a Política de Segurança e Inteligência Institucional - Implantar iniciativas de conscientização acerca do tratamento de conteúdos sensíveis - Implementar a Política de Proteção de Dados da Segurança de Controle de Acesso - Elaborar relatório de riscos das atividades de segurança institucional

OE	INICIATIVAS ESTRATÉGICAS
14 Gestão Documental	- Definir requisitos para a gestão, preservação e acessibilidade da documentação digital - Implantar protocolo e sistema eletrônico integrado
15 Gestão Administrativa	- Racionalizar recursos logísticos, financeiros e de TI, com foco em sustentabilidade, segurança e efetividade
19 Governança de Dados	- Promover a governança e gestão de dados, de forma a institucionalizar a coleta, o tratamento, a análise, o controle, a utilização, a integração, a segurança e a disseminação de dados internos e externos (sensíveis e classificados) - Desenvolver competências para promover a alfabetização digital e a inovação
25 Atuação Criminal	- Estruturar a atuação na prevenção e enfrentamento dos crimes cibernéticos, com a utilização de ferramentas de tecnologia, análise e interpretação de grandes volumes de dados, estruturados ou não estruturados

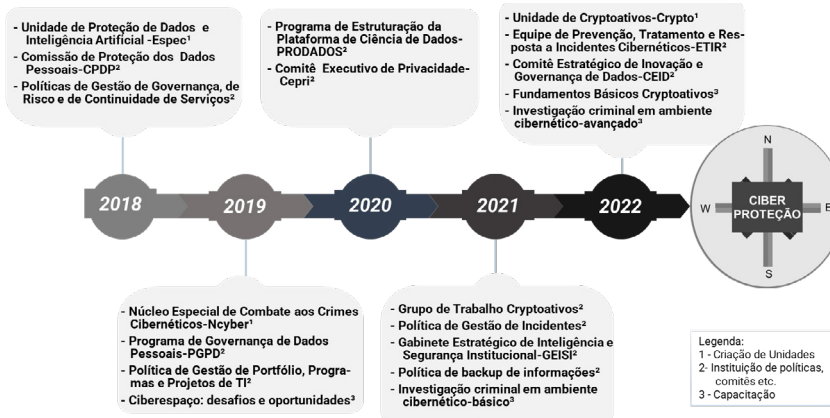
Fonte: Elaborado pelo autor.

Extrapolando positivamente as ações previstas, a campanha do lixo eletrônico de 2022, realizada entre 16 de maio e 10 de junho, que rendeu 139 kg de resíduos para descaracterização e reciclagem, exemplifica a sintonia entre planejamento (OE 5) e execução no âmbito do MPDFT. O descarte seguro do lixo eletrônico (digital) vem crescendo em importância nas últimas duas décadas e será abordado mais adiante, em conjunto com a preservação digital.

A Figura 3 busca sintetizar, cronologicamente, em sintonia com o PEI e sob o filtro alargado da Ciber Proteção, algumas das

mais relevantes iniciativas do MPDFT de 2018 até meados do segundo semestre de 2022.

Figura 3 – O MPDFT e a Ciber Proteção – iniciativas



Fonte: Elaborado pelo autor.

Nota-se que o acompanhamento evolutivo do cenário cibernético nacional resultou também na aglutinação e extinção de algumas iniciativas anteriores. Exemplificando, com a criação da Crypto[6], no corrente ano, foram extintas: a Comissão de Direito Digital (CODD), a Comissão de Proteção dos Dados Pessoais e a Unidade Especial de Proteção de Dados e Inteligência Artificial (Espec), assim como com a instituição do Comitê

[6] Dentre as competências da Crypto destacam-se: (i) promover ações informativas que orientem a população do Distrito Federal e do restante do país sobre o uso seguro, ponderado e responsável dos cryptoativos; (ii) gerir e operar ferramentas de rastreamento e monitoramento de ativos nas *blockchains*; e (iii) operacionalizar o Projeto CRYPTO, que objetiva criar o primeiro laboratório de lavagem de dinheiro por meio de cryptoativos do Brasil.

Estratégico de Inovação e Governança de Dados, foi extinto o Comitê de Privacidade.

Ilustrando os desdobramentos das iniciativas, encontram-se em curso a adesão à Rede Federal de Gestão de Incidentes Cibernéticos pela Equipe de Prevenção, Tratamento e Resposta a Incidentes de Redes (ETIR\MPDFT) e as etapas de identificação das bases de dados e capacitação de pessoas do Programa de Governança de Dados Pessoais.

A próxima seção complementa a abordagem iniciada neste trabalho, propondo alguns subsídios para o aprimoramento da proteção cibernética.

3 Contribuições para a consolidação da Ciber Proteção no MP

O uso seguro do espaço cibernético de interesse envolve fatores diversos e, por vezes, interdependentes, assim, as seções seguintes sugerem algumas *melhores práticas* para a consolidação e a evolução sistêmica, em particular sobre os aspectos relacionados à proteção dos dados pessoais, segurança cibernética, capacitação cibernética do cidadão e preservação digital.

3.1 Maturidade na proteção de dados pessoais

Ampliar a utilização de dados nas tomadas de decisão é um dos fatores que conduz à excelência no cumprimento da missão institucional. Nessa direção, proporcionar acesso seguro dos integrantes do MP e do público externo aos sistemas informacionais,

assim como salvaguardar e preservar os repositórios de dados institucionais fazem parte do escopo da Ciber Proteção.

Compõem este quadro os dados que possibilitem a identificação, direta ou indireta, da pessoa natural, que devem ser tratados de forma alinhada com a Lei Geral de Proteção de Dados Pessoais (LGPD).

No processo de adequação da LGPD na Instituição, cresce de relevância avaliar a maturidade da implementação da Lei. A própria LGPD, no art. 50, propõe a formulação de regras de boas práticas e de governança pelos agentes de tratamento, assim como a implementação de um programa interno de governança em privacidade que, no mínimo:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

g) conte com planos de resposta a incidentes e remediação; e

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas. (BRASIL, 2018b).

Segundo Nery (2022), uma avaliação de maturidade tem diversos objetivos e benefícios, tais como:

a) Alinhar a conformidade da LGPD com o negócio, definindo a maturidade desejada em cada requisito da Lei;

b) Avaliar o grau de conformidade, facilitando perceber os gaps de maneira qualitativa;

c) Criar linguagem comum e facilitar a comunicação, particularmente do Encarregado com o ambiente interno e o público externo;

d) Decidir em bases mais sólidas, provendo maior consistência às deliberações acerca da evolução no processo de conformidade, bem como direcionando melhor o uso dos recursos;

e) Aumentar o conhecimento, engajamento e conscientização institucional sobre o tema;

f) Fortalecer a *prestação de contas*, incluindo controle interno e auditorias; e

g) Apoiar o planejamento e justificar investimentos, por meio da adoção de indicadores efetivos.

A avaliação de maturidade deve começar após o projeto de implementação ou com a implementação em estágio avançado, devendo ser feita de forma independente e contínua.

Entre as referências que podem alavancar a maturidade organizacional sobre o tema, sobressai a compilação realizada pela Secretaria de Governo Digital do Ministério da Economia, nomeadamente o *Guia do Framework de Segurança: Lei Geral de Proteção de Dados Pessoais (LGPD)*, revisado em janeiro de 2022 (BRASIL, 2022).

Os assuntos de boas práticas e governança estão contidos no Capítulo VII da LGPD, que aborda também a temática da segurança, objeto da seção que se segue.

3.2 Gestão de incidentes cibernéticos

Além de a crise sanitária mundial incrementar o uso do espaço cibernético individualmente ou de forma corporativa, vem proporcionando alterações nos modelos de trabalho, tanto no setor público quanto no privado. Percebe-se o incremento de práticas mais flexíveis, como a realização de atividades por meio de acesso remoto, especialmente por colaboradores e prestadores de serviço, influenciando também o emprego das tecnologias de informação e de comunicação.

Desde meados de 2020, permanece acelerada a implementação de novas funcionalidades, como a adoção de soluções em *nuvem* e de trabalho cooperativo a distância. Somam-se às consequências nefastas da recente pandemia, na perspectiva da Ciber Proteção, a expansão da superfície de ataque externa das organizações e a fragilização do fator humano como usuário de sistemas informatizados.

O cenário crescente de ameaças deve permanecer, particularmente em relação aos ataques de sequestro de dados, como demonstra a empresa WatchGuard[7]. Tais fatos corroboram a necessidade imediata de ajustes nas medidas de proteção adotadas, com ênfase na segurança corporativa.

A segurança cibernética pode ser organizada em diversas etapas, desde o levantamento dos ativos de informação (pessoas, *hardware*, *software*, dados e processos), correção de vulnerabilidades, estabelecimento de medidas de proteção e detecção de ações adversas, até o tratamento de incidentes.

Particularmente em relação à gestão de incidentes cibernéticos, torna-se imprescindível que as organizações públicas e privadas disponham de uma equipe dedicada, com especializações específicas, conhecidas internacionalmente como *Computer Security Incident Response Team* (CSIRT).

[7] De acordo com o Internet Security Report, o volume de *ransomware* no final do primeiro trimestre de 2022 já dobrou em comparação com o total de 2021. Informações adicionais disponíveis em: https://itforum.com.br/noticias/2022-deve-quebrar-recorde-de-deteccoes-de-ransomware/.

No Brasil, os CSIRTs são denominados Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIRs) e podem contar com o apoio técnico do CERT.br, do CTIR Gov e do CAIS/RNP (vide seção 1.1).

Em termos de implantação, aperfeiçoamento e avaliação de maturidade de uma ETIR, seria oportuno utilizar complementarmente dois guias: (i) o *Framework de Segurança*, sugerido na seção anterior, particularmente o "CIS Controle 17: Gestão de resposta a incidentes"; e o (ii) *Guia de aperfeiçoamento da segurança cibernética para as infraestruturas críticas*, disponibilizado pelo National Institute of Standards and Technology, em especial as funções "Responder e Recuperar" do *Cybersecurity Framework*. A função Responder abrange a contenção do impacto de um incidente, contemplando: planejamento de resposta, notificações, análise, mitigação e aperfeiçoamentos decorrentes; enquanto a função Recuperar trata da implementação de planos de resiliência, restauração de recursos prejudicados e retomada de serviços interrompidos pelo incidente (U.S. CHAMBER OF COMMERCE, 2018).

Especial atenção deve ser dedicada às iniciativas do setor público, como o alinhamento das políticas e estratégias (vide seção 1.2) e, em termos operacionais, a adesão à Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC).

A ReGIC busca aprimorar a coordenação entre os mais diversos órgãos e seguimentos na gestão dos incidentes cibernéticos e, dentre os seus objetivos, destacam-se:

a) Divulgar medidas de prevenção, tratamento e resposta a incidentes cibernéticos;
b) Compartilhar alertas sobre ameaças e vulnerabilidades cibernéticas;
c) Divulgar informações sobre ataques cibernéticos;
d) Promover a cooperação entre os participantes da Rede; e
e) Promover a celeridade na resposta a incidentes cibernéticos (BRASIL, 2021a).

Como percebido anteriormente, o aumento do trabalho remoto, e o consequente uso das redes domésticas e dos equipamentos pessoais (*home office*), ampliou os alvos dos ataques cibernéticos para além do ambiente tecnológico das empresas. Tal fato *de per si* evidencia a urgência na melhoria do preparo individual, a ser aprofundado na próxima seção, sob a visão multifacetada da literacia digital.

3.3 Literacia digital

O fator humano sempre foi relevante no processo da Ciber Proteção quanto às práticas diárias dos ambientes privado e público. Entretanto, em tempos hodiernos e pandêmicos, vem acontecendo uma aceleração no uso do meio digital, em especial das mídias de relacionamento social e da internet como ambiente de realização de tarefas cotidianas, tais como: compra de produtos, pedido de alimentação, utilização de serviços públicos etc. Tal incremento abrupto e em larga escala amplifica os riscos cibernéticos individuais.

A crescente interação com as *novas* mídias (blogues, imprensa digital, mídias sociais, metaverso, entre outros) requer, resumidamente, a capacidade de: (i) filtrar as informações; (ii) interpretar o significado das mensagens; e (iii) verificar a veracidade dos dados. Em complemento, exemplos de deveres e direitos do cidadão, como votar nas urnas eletrônicas ou interagir com a plataforma do governo digital, extrapolam a necessidade de simples compreensão instrumental no manuseio de aplicativos e de dispositivos eletrônicos.

Neste cenário, aflora o número de ameaças que têm como origem o uso de engenharia social[8] e urge aprofundar não somente habilidades, mas consolidar conhecimentos e atualizar competências cibernéticas, ou seja, alavancar a literacia digital no seio da sociedade brasileira.

A American Library Association (ALA) define literacia digital como:

> a capacidade de usar tecnologias de informação e comunicação para encontrar, avaliar, criar e transmitir informações, exigindo habilidades cognitivas e técnicas. Como a alfabetização informacional, a literacia digital requer habilidades na localização e uso de informações e no pensamento crítico. […] envolve conhecer ferramentas digitais e usá-las de forma comunicativa e colaborativa por meio do engajamento social. (ALA, 2022, tradução nossa).

[8] Ataques de acesso que tentam manipular pessoas para tomar ações (por exemplo: clicar em arquivos com artefatos maliciosos) ou divulgar informações sensíveis (que controlam o acesso aos sistemas e redes) e, por meio delas, invadir contas e/ou dispositivos corporativos. Exemplo concreto e de grande envergadura pode ser encontrado em: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.

Cunha e Cavalcanti (2008) associam literacia digital com a alfabetização informacional e a tecnológica. Assim, pode-se compilar o termo como um conjunto de competências elementares que uma pessoa possui para identificar, manipular, elaborar estratégicas de busca, localizar a informação, bem como avaliar as suas fontes, especialmente no uso de qualquer tecnologia de informação e de comunicação, como os serviços de internet.

A Organização das Nações Unidas para a Educação, a Ciência e a Cultura (Unesco), de forma análoga, entende literacia digital como alfabetização, no caso, das mídias e informacional (AMI), propondo cinco leis básicas:

a) Lei 1: bibliotecas, mídias, internet, bem como outras formas de provedores de informação, são para uso em engajamento cívico crítico e desenvolvimento sustentável. Eles são iguais em estatura e nenhum é mais relevante que o outro;

b) Lei 2: todo cidadão é um criador de informação/conhecimento e tem uma mensagem. Eles devem ser capacitados para acessar novas informações/conhecimentos e se expressar;

c) Lei 3: informação, conhecimento e mensagens nem sempre são neutras em termos de valor, ou sempre independentes de preconceitos, essa verdade deve ser repassada de forma transparente e compreensível para todos os cidadãos;

d) Lei 4: todo cidadão quer conhecer e compreender novas informações, conhecimentos e mensagens, bem como se comunicar, mesmo que não tenha conhecimento, admita

ou expresse que o faz. Seus direitos, no entanto, nunca devem ser comprometidos;

e) Lei 5: a alfabetização midiática e informacional (literacia digital) não é adquirida de uma só vez. É uma experiência e um processo vivido e dinâmico, incluindo conhecimentos, habilidades e atitudes (UNESCO, 2018).

A literacia digital também pode ser entendida como uma competência para a cidadania ou *emancipação cibernética*, favorecendo a alocação no mercado de trabalho e mitigando o analfabetismo funcional, particularmente pela capacidade de elaboração sobre conteúdos, formação de redes e conexão em espaços colaborativos.

A literacia digital, em sentido lato e no contexto da Ciber Proteção, reduz o descompasso entre a evolução das tecnologias de informação e o preparo do cidadão para a utilizá-las *de forma segura no meio digital*, bem como, a depender do uso do espaço cibernético, propiciando a possibilidade de:

a) Limitar os efeitos da desinformação[9], ao ampliar a capacidade de o indivíduo acessar, avaliar criticamente, compreender e ainda criar mídias;

b) Aumentar o nível de autonomia e de segurança na navegação pelo espaço cibernético, nomeadamente no

[9] A depender da conjuntura, a desinformação pode conter uma ou mais das seguintes características: (i) a informação ser falsa ou levar a falsas conclusões; (ii) capacidade de confundir e induzir ao erro; (iii) ser compartilhada de forma deliberada, com intenção de enganar; e (iv) informar mal, suprimindo informações, diminuindo sua importância ou modificando o seu sentido.

acesso a sítios *web* de real valia, no estabelecimento de estratégias de busca e na interação com as mídias sociais;

c) Aprimorar as competências para evitar fraudes, exposição de conteúdos sensíveis e armadilhas nos relacionamentos sociais; e

d) Evitar as armadilhas e ações de engenharia social, reduzindo os efeitos dos artefatos maliciosos de forma geral.

Entende-se que o aperfeiçoamento da literacia digital é questão de Estado, devendo ser proporcionado a todos os seguimentos da sociedade brasileira, com senso de urgência e de forma contínua.

Fechando as contribuições, a próxima seção abordará a temática da preservação digital institucional, com destaque para o descarte seguro do lixo digital.

3.4 Preservação e o descarte digital

Para Vint Cerf, considerado *um dos pais da Internet*, a preservação é uma questão fundamental que pode afetar o futuro da Internet, levando a uma situação de perda de memória, a qual denominou de *a era negra da Internet*. O cocriador do protocolo TCP/IP aponta que a longevidade do mundo digital está diretamente relacionada à capacidade de preservação de arquivos, pois acredita-se que os *bits* são indestrutíveis. No seu entendimento, diversas atividades, como a definição de um padrão mundial de documentos digitais que perdure por décadas, já deveriam estar

em curso, de forma global e cooperativa (WORLD CONGRESS ON INFORMATION TECHNOLOGY, 2016).

Tais observações vêm reforçar a relevância de uma abordagem interativa, envolvendo segurança no espaço cibernético, informação e preservação digital (PD).

Na conjuntura da gestão documental brasileira, em 2015, o Conselho Nacional de Arquivos (Conarq) aprovou as Diretrizes para a Implementação de Repositórios Arquivísticos Digitais Confiáveis (RDC-Arq), no que tange ao arquivamento e à manutenção dos documentos arquivísticos em formato digital em todo o seu ciclo de vida. Dessa forma, o Conarq busca garantir: "a autenticidade (identidade e integridade), a confidencialidade, a disponibilidade e a *preservação* desses documentos" (CONARQ, 2015, p. 3, grifo nosso), tendo em vista a perspectiva da necessidade de manutenção dos acervos documentais por longos períodos ou, até mesmo, permanentemente.

No contexto de um RDC-Arq, entende-se *preservação* como um conjunto de práticas imprescindíveis ao funcionamento administrativo da organização que produziu a informação (documento) digital, assim como base fundamental para a manutenção de sua memória e patrimônio cultural, devendo compor o ecossistema da proteção cibernética institucional (VIANNA, 2019).

Assim, particularmente impulsionado pela migração irreversível dos processos judiciais para o eletrônico/digital e pela necessidade de salvaguardar a memória institucional, cabe ao Ministério Público empreender esforços no aperfeiçoamento

das suas estruturas imbricadas com a preservação digital. Nesse sentido, o MP pode dispor do auxílio da Rede Brasileira de Serviços de Preservação Digital (Cariniana)[10], inclusive para atualização da política de preservação digital institucional.

Extinta a serventia do objeto informacional, encerra-se o processo de preservação com o descarte, que pode ser do suporte físico (mídias) ou apenas lógico (*bits*)[11].

Para os objetivos deste trabalho, destaca-se o processo de *descarte digital*, ou seja, dos dados e informações contidas no lixo eletrônico físico como computadores, mídias de *backup*, *pen drives*, celulares etc. Importa ainda o lixo digital – as informações inúteis – armazenado nos sistemas e aplicações localizados em infraestrutura própria ou na *nuvem*, como portais da *web* e repositórios de dados, entre outros.

Considerando-se que *a lixeira de um homem é o tesouro de outro*, o descarte inadequado do lixo digital facilita a obtenção de informações sensíveis ou confidenciais pelos engenheiros sociais, que podem explorar as vulnerabilidades encontradas no *lixo* pessoal ou institucional, facilitando o planejamento e a execução de ataques cibernéticos.

---

10 A Rede Cariniana surgiu da necessidade de se criar, no Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT), uma rede de serviços de preservação digital de documentos eletrônicos brasileiros. Informações adicionais disponíveis em: https://www.gov.br/ibict/pt-br/assuntos/informacao-cientifica/cariniana.

11 Ressalva-se que o descarte digital de um objeto informacional armazenado em um repositório institucional deve ser realizado de forma periódica, criteriosa e segura por profissional da informação especializado em PD.

O desafio consiste em apagar o refugo de forma permanente e não apenas restringindo o acesso, como acontece no caso das *lixeiras* existentes nos sistemas operacionais, que deixam trilhas nos dispositivos de armazenamento dos computadores. Convém, por vezes, o uso de aplicativos específicos que substituem os dados repetidas vezes por zeros e uns, dificultando o êxito de ferramentas forenses de recuperação de arquivo. A depender da sensibilidade dos dados, a melhor maneira de garantir que arquivos não sejam recuperáveis é destruir fisicamente o dispositivo de armazenamento.

A preparação do lixo eletrônico para descarte também deve ser realizada individualmente, tanto no ambiente corporativo como no doméstico. Ao se levar o equipamento para reciclagem, deve ter-se em consideração que ele poderá conter arquivos sensíveis pessoais ou mesmo da organização, tais como: declarações de imposto de renda, extratos bancários, prescrições e exames médicos, rascunhos de projetos, balanços financeiros, análise de documentos, mapeamento de ações futuras etc.

Cabe ressaltar que, mesmo que o descarte seja realizado por intermédio de uma empresa especializada e/ou contratada, não há a garantia de que ele seja seguro. O lixo digital deve ser tratado de forma especial antes de ser entregue, como prevê o Decreto nº 10.240, que regulamenta a implementação de sistema de logística reversa de produtos eletroeletrônicos e seus componentes de uso doméstico. O próprio decreto, reforça, no inciso II, do seu art. 31, que é obrigação dos consumidores "remover, previamente

ao descarte, as informações e os dados privados e os programas em que eles estejam armazenados nos produtos eletroeletrônicos, discos rígidos, cartões de memória e estruturas semelhantes, quando existentes" (BRASIL, 2020a).

4 Desdobramentos e conclusões

Acredito que uma das poucas unanimidades contemporâneas aponta para uma sociedade mundial organizada em rede, utilizando-se do espaço cibernético como vetor de sustentabilidade, desenvolvimento e integração global, favorecendo a autonomia e o equilíbrio entre países e nações, bem como a estabilidade de economias com representatividade nacional.

Neste ambiente em expansão, cada Estado-Nação organiza, fortalece e protege seu ecossistema digital, a fim de exercer plenamente sua soberania, seja preservando direitos individuais, seja implementando políticas e ações em prol da sociedade ou da defesa nacional.

Não obstante, a manutenção, simplificação e ampliação da relação do poder público com a sociedade, por meio do uso das tecnologias, aprimoram as conquistas do cidadão, exigindo um esforço multidisciplinar e coordenado para protegê-las.

Dentre os entendimentos abordados neste trabalho e nos muitos desafios ainda por vir, finalizo destacando duas reflexões a serem debatidas em futuro contíguo.

4.1 Primeira reflexão

Considerando que os sistemas essenciais para sustentar a sociedade contemporânea, como as infraestruturas críticas urbanas, têm sido cada vez mais digitalizados, dependentes de computadores e redes (incluindo a internet) para operar, estando cada vez mais interligados e sob ataque;

Considerando que a adoção de novas redes 5G e o uso massivo da internet das coisas (IOT) favorecem a consolidação das cidades inteligentes no país (*smart cities*), expondo ainda mais os cidadãos a ameaças cibernéticas;

Considerando a vocação de Brasília como cidade digital de destaque no Distrito Federal e no cenário cosmopolita;

Considerando que falhas nas medidas de proteção comprometem a segurança e o funcionamento dos sistemas digitais, podendo resultar em catástrofe tais como interrupções de serviços e sequestro de dados (vide caso Baltimore/2019); indaga-se:

– Em que circunstâncias e com quais procedimentos poderia o Ministério Público atuar no enfrentamento de crise severa nas infraestruturas críticas urbanas?

4.2 Segunda reflexão

Considerando a importância do fator humano para a Ciber Proteção nacional;

Considerando que no ecossistema da Ciber Proteção é vital que a população brasileira possua elevada capacitação cibernética,

a fim de não somente fazer usufruto seguro de toda a potencialidade dos sistemas informacionais disponibilizados e da internet de forma geral; mas também contribua para a salvaguarda do espaço cibernético de relevância nacional;

Considerando o incremento da cultura cibernética para a prosperidade do país;

Considerando a universalidade de acesso à prestação digital dos serviços públicos, possibilitando a ampliação de direitos e oportunidades e favorecendo a redução de custos do cidadão e institucionais;

– De que maneira poderia o Ministério Público participar mais ativamente no aperfeiçoamento da literacia digital do cidadão?

A fim de permanecer atuando no cenário nacional cibernético, o Ministério Público deve acompanhar as tendências tecnológicas e as evoluções normativas, bem como necessita manter postura flexível e inovadora na administração de seus recursos pessoais e materiais.

A consolidação e o aprimoramento da Ciber Proteção institucional é fator de sucesso na ampliação do escopo de atuação do MP no espaço cibernético de interesse e devem ser realizadas concomitantemente com ações externas, com equilíbrio entre as iniciativas, particularmente na alocação de recursos financeiros e de pessoal.

Portanto, seu aprimoramento urge ser orgânico e dinâmico, envolvendo pessoas, processos, estruturas tecnológicas e

normatização, devendo também considerar a interdependência entre os fatores envolvidos e a avaliação periódica do próprio ecossistema digital.

Title: Cyber Protection and the Public Prosecution Office: interfaces and prospects

Abstract: The importance of the dominance of the cybernetic space to the contemporaneous society is notorious, and each Nation-State is responsible for organizing, strengthening, and protecting its digital ecosystem to fully exercise its sovereignty, whether preserving individual rights or implementing policies and actions for the benefit of the society or the national defense. This article presents the concept of Cyber Protection as a complex ecosystem which covers activities in the areas of digital information security, cyber defense, digital preservation, and critical infrastructures; and lists the main actors of national cyber security and defense. The national regulatory framework is reviewed in search of updated guidelines on the broad context of digital information protection. Then, it discusses the initiatives of the Public Prosecution Office of the Federal District and Territories, such as updating its strategic planning, implementing units and establishing committees and programs under the perspective of Cyber Protection. It is understood that the promotion of citizenship and justice by the Public Prosecution Office must be in constant improvement, especially in the cybernetic sphere, contemplating the safe use of digital media by Brazilian society. As a result, it details possible contributions and questions in favor of the maturity in data protection, incident management, citizen cyber empowerment, and digital disposal.

Keywords: Cyber space. Cyber protection. Cyber security. Digital information security.

Referências

AMERICAN LIBRARY ASSOCIATION (ALA). *Digital literacy*. Chicago: ALA, c2022. Disponível em: https://literacy.ala.org/digital-literacy/. Acesso em: 19 jul. 2022.

BANCO CENTRAL DO BRASIL (BCB). *Moedas virtuais*. Brasília, DF: BCB, 2020. Disponível em: https://www.bcb.gov.br/acessoinformacao/perguntasfrequentes-respostas/faq_moedasvirtuais. Acesso em: 16 jul. 2022.

BRASIL. Decreto nº 9.573, de 22 de novembro de 2018. Aprova a Política Nacional de Segurança de Infraestruturas Críticas. *Diário Oficial da União*, Brasília, DF, 23 nov. 2018a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm. Acesso em: 19 jul. 2022.

BRASIL. Decreto nº 10.748, de 16 de julho de 2021. Institui a Rede Federal de Gestão de Incidentes Cibernético. *Diário Oficial da União*, Brasília, DF, 19 jul. 2021a. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.748-de-16-de-julho-de-2021-332610022. Acesso em: 19 jul. 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*, Brasília, DF, 15 ago. 2018b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 jul. 2022.

BRASIL. Ministério da Defesa. Portaria nº 3.781/GM-MD, de 17 de novembro de 2020. Cria o Sistema Militar de Defesa Cibernética (SMDC) e dá outras providências. *Diário Oficial da União*, Brasília, DF, 19 nov. 2020b. Disponível em: https://portal.in.gov.br/en/web/dou/-/portaria-n-3.781/gm-md-de-17-de-novembro-de-2020-289248860. Acesso em: 19 jul. 2022.

BRASIL. Ministério da Economia. *Guia do Framework de Segurança*: Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Ministério da Economia, 2022. Versão 2.0. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_framework_seguranca.pdf. Acesso em: 19 jul. 2022.

BRASIL. Senado Federal. *Projeto de Lei nº 4401/2021 (nº 2.303/2015, na Câmara dos Deputados)*. Brasília, DF: Senado Federal, 2021b. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9054002&ts=1653562815393&disposition=inline. Acesso em: 15 jul. 2022.

CONSELHO NACIONAL DE ARQUIVOS (CONARQ). *Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis:* RDC-Arq. Rio de Janeiro: Conarq, 2015. Disponível em: https://www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/conarq_diretrizes_rdc_arq_resolucao_43.pdf. Acesso em: 23 jul. 2022.

CUNHA, Murilo Bastos da; CAVALCANTI, Cordélia Robalinho de Oliveira. *Dicionário de biblioteconomia e arquivologia.* Brasília, DF: Briquet de Lemos, 2008. Disponível em: https://repositorio.unb.br/handle/10482/34113. Acesso em: 16 jul. 2022.

ISHIKAWA, Edison *et al*. Modeling a cyber defense business ecosystem of ecosystems: nurturing Brazilian cyber defense resource. In: INFORMATION RESOURCES MANAGEMENT ASSOCIATION (ed.). *Research anthology on business aspects of cybersecurity.* Hershey: IGI Global, 2022. p. 649-675.

MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS (MPDFT). *Planejamento Estratégico Institucional (PEI 2022-2026)*. Brasília, DF: MPDFT, 2022. Disponível em: https://www.mpdft.mp.br/portal/images/planejamento_estrategico/PEI_documento_13_10_2022.pdf. Acesso em: 19 jul. 2022.

NERY, Fernando. *Benefícios da avaliação de maturidade.* [S. l.], 22 jul. 2022. LinkedIn: Bom dia LGPD. Disponível em: https://www.linkedin.com/pulse/benef%25C3%25ADcios-da-avalia%25C3%25A7%25C3%25A3o-de-maturidade-fernando-nery/?trackingId=9n%2F04vQhkRS%2BuVZGuMvtBw%3D%3D. Acesso em: 16 jul. 2022.

ORTIZ, Jorge L. 'Soft targets': beleaguered Baltimore still reeling from a cyberattack. And that's just its latest woe. *USA Today*, McLean, 24 May 2019. Disponível em: https://www.usatoday.com/story/news/nation/2019/05/24/hackers-hit-vulnerable-cities-like-baltimore-ransomware-attacks/1211611001/. Acesso em: 10 jul. 2022.

UNESCO launches five laws of media and information literacy (MIL). Unesco Almaty, Almaty, 19 Dec. 2018. Disponível em: http://en.unesco.kz/unesco-launches-five-laws-of-media-and-information-literacy-mil. Acesso em: 31 jul. 2022.

U.S. CHAMBER OF COMMERCE. *Guia de aperfeiçoamento da segurança cibernética para as infraestruturas críticas.* Washington, DC: Brazil-U.S. Business Council, 2018. Disponível em: https://www.uschamber.com/assets/archived/images/intl_nist_framework_portugese_finalfull_web.pdf. Acesso em: 12 jul. 2022.

VIANNA, Eduardo Wallier. *Segurança da informação digital:* proposta de modelo para a Ciber Proteção nacional. 2019. Tese (Doutorado em Ciência da Informação) – Universidade de Brasília, Brasília, DF, 2019. Disponível em: https://repositorio.unb.br/handle/10482/35253. Acesso em: 12 jul. 2022.

WORLD CONGRESS ON INFORMATION TECHNOLOGY, 20., 2016, Brasília, DF. *Anais* […]. Brasília, DF: The Brazilian Federation of Information Technology Companies, 2016. Disponível em: http://www.wcit2016.org/. Acesso em: 18 out. 2016.

Referência bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

VIANNA, Eduardo Wallier. Ciber Proteção e o Ministério Público: interfaces e prospectivas. *Revista do Ministério Público do Distrito Federal e Territórios,* Brasília, n. 12, p. 249-290, 2022. Anual.
