Relatório do workshop

“Serviços essenciais, teletrabalho e segurança da informação em tempos de exceção”

1. Informações básicas sobre o Workshop:

• Título e tema do Workshop: “Serviços essenciais, teletrabalho e segurança da informação em tempos de exceção” realizado dia 23/09/2020.
• Formato (painel, mesa redonda ou debate; outro formato): Painel
• Proponentes e co-proponentes:

Proponente: **Mariana Canto**

UF	PE
Organização	Instituto de Pesquisa em Direito e Tecnologia do Recife - IP.rec
Setor	Comunidade Científica e Tecnológica

Co-proponente: **Gustavo Ramos Rodrigues**

UF	MG
Organização	Instituto de Referência em Internet e Sociedade - IRIS
Setor	Terceiro Setor

- **Palestrante: Rita de Castro Hermes Meira Lima**

Organização	Defensoria Pública do Distrito Federal/DPDF e Associação Nacional das Defensoras e Defensores Públicos/ANADEP
Setor	Governamental

Mini biografia
Coordenadora do Núcleo de Promoção e Defesa dos Direitos das Mulheres da DPDF; Membro da Comissão da Mulher da ANADEP. Mestre em Direito e Políticas Públicas pelo UNICEUB. Pós graduanda em Direito e Gênero pela Escola da Magistratura do Distrito Federal.

- **Palestrante: Gustavo Ramos Rodrigues**

Organização	Instituto de Referência em Internet e Sociedade - IRIS

Setor Terceiro Setor

Mini biografia

Pesquisador no Instituto de Referência em Internet e Sociedade. Mestrando em Divulgação Científica e Cultural pela Unicamp. Bacharel em Antropologia pela UFMG.

- Palestrante: Mariana Canto

UF PE

Organização Instituto de Pesquisa em Direito e Tecnologia do Recife - IP.rec

Setor Comunidade Científica e Tecnológica

Mini biografia

Pesquisadora do Instituto de Pesquisa em Direito e Tecnologia do Recife - IP.rec. Formada em Direito pelo Centro de Ciências Jurídicas da Universidade Federal de Pernambuco.

- Palestrante: Dario Carnevalli Durigan

UF SP

Organização Facebook Brasil

Setor Empresarial

Mini biografia

Law Enforcement Outreach Manager do Facebook na América Latina. Responsável por desenvolver e manter relacionamentos estratégicos com as autoridades policiais e agências governamentais relacionadas à família de aplicativos (incluindo Facebook, Instagram, WhatsApp e Oculus), com foco na segurança e proteção da Internet, e coalizões relacionadas ao setor no Brasil e em outros países na LatAm.

• Moderador(a): Leonardo Ribeiro da Cruz

UF PA

Organização Universidade Federal do Pará

Setor Comunidade Científica e Tecnológica

Mini biografia

Doutor em sociologia pela Unicamp, com pós doutorado no Laboratório de Estudos Avançados em Jornalismo (LabJor/Unicamp). Professor Adjunto de Teoria Sociológica da Universidade Federal do Pará. Professor Permanente do Programa de Pós-Graduação

em Sociologia e Antropologia (PPGSA/UFPA). Coordenador do Laboratório Amazônico de Estudos Sociotécnicos da UFPA (laesufpa.net) e pesquisador da Rede Latino

• **Relator(a): Janaina Spode**

UF	RS
Organização	Casa da Cultura Digital Porto Alegre - CCDPOA
Setor	Terceiro Setor

Mini biografia

É integrante da Casa da Cultura Digital Porto Alegre, um coletivo de ativistas, profissionais e pesquisadores fundado em 2012, focado em tecnopolítica e direitos digitais e atua como Digital Security Specialist no ISC Project Brazil. Nacionalmente atua também com a Coalizão Direitos na Rede na luta pelos direitos humanos e pela manutenção da privacidade e da Internet livre e aberta.

2. Estruturação do Workshop

• Objetivos e resultados (propostos e atingidos):

- Objetivos:

Pretende-se abordar a migração, devido às políticas de quarentena, dos serviços essenciais à sociedade para as plataformas online e, consequentemente, a relevância dos recursos de cibersegurança. Busca-se debater sobre a inauguração de canais emergenciais de funcionamento via aplicativos - desde o teletrabalho ao funcionamento de Defensorias Públicas, Procons e delegacias, entre outros - sob a perspectiva dos recursos críticos que asseguram o sigilo, a autenticidade e a disponibilidade das comunicações desses serviços. O painel, portanto, irá propor exposições sobre como a criptografia, nesse contexto, se reafirma enquanto elemento central à segurança da rede e à confiabilidade nas plataformas online.

Será posta em perspectiva a construção legislativa, jurídica e política brasileira relativa à criptografia. De um lado, são sedimentadas bases legais e recomendações de boas práticas que promovem a adoção de medidas de segurança para o desenvolvimento tecnológico. Entre elas, a Política Nacional de Segurança da Informação; a Estratégia Nacional de Segurança Cibernética; o Decreto nº 8771, a Lei Geral de Proteção de Dados; bem como os Princípios para o Uso e Governança da Rede no Brasil do CGI.br.

De outro, questões de caráter contextual e político, tal como o Projeto de Lei nº 9.808 (procura criar mecanismos de acesso à chave criptográfica por parte de agências de investigação); as ações em trâmite no Supremo Tribunal Federal, em especial a ADPF nº 403; e a geopolítica em torno da criação de mecanismos de acesso excepcional às comunicações encriptadas.

Na medida em que a criptografia se apresenta enquanto elemento fundamental à segurança e resiliência da rede, será proposta a reflexão sobre até que ponto plataformas de criptografia se tornam essenciais para o funcionamento de serviços públicos e privados básicos. Portanto, a partir de uma construção multissetorial, pretende-se debater sobre como o cenário gerado pela Covid-19 revoluciona essas correlações.

- Resultados:

O workshop possibilitou uma discussão qualificada a respeito da importância da cibersegurança e da criptografia em um cenário de crescimento do acesso e uso da Internet como é o caso do Brasil, como também mobilizou o interesse público em relação ao tema através das perguntas realizadas. Baseado em exemplos práticos e expertises de cada um dos debatedores, o encontro de representantes de diferentes setores brasileiros junto ao debate possibilitado pela interação com a audiência presencial e remota contribuiu com debates pré-existentes, como aqueles no âmbito do judiciário e do legislativo brasileiro, uma vez que ainda há a escassez de reflexões acerca da importância de políticas de segurança relacionadas à oferta de serviços, essenciais ou não, na modalidade digital, tanto na esfera pública como na esfera privada.

• Justificativa em relação à governança da Internet:

A segurança da informação é um tema crucial para a governança da internet. Ela é afirmada no âmbito do princípio de funcionalidade, segurança e estabilidade, reiterado em instrumentos como a Declaração Multissetorial do NETmundial e a Resolução CGI.br/RES/2009/003/P. Além de constituir um valor para a governança em si mesma, a segurança da informação é condição para o respeito efetivo a diversos outros princípios, a exemplo de diversidade, liberdade, privacidade e direitos humanos. No próprio Fórum da Internet no Brasil, a tópica tem sido abordada com frequência, tanto em workshops especificamente voltados a temas securitivos - como criptografia e direitos humanos - quanto em atividades que versam sobre questões adjacentes, como proteção de dados pessoais, vigilância e regulação. No VII FIB, a cibersegurança foi, inclusive, tema de sessão plenária. Trata-se, portanto, de um tema inerentemente relevante, porém cuja

importância foi ainda mais notabilizada no contexto da pandemia de COVID-19, ocasião em que diversas atividades realizadas presencialmente passaram a ser operadas em âmbito digital. Destaca-se, nessa seara, o uso massivo de plataformas de videoconferências, as quais passaram a ser empregadas inclusive para a realização de sessões plenárias no Congresso Nacional e no Supremo Tribunal Federal. Tal cenário aumenta a urgência do debate sobre cibersegurança e criptografia, uma vez que a digitalização dessas atividades vulnerabiliza cidadãos e instituições à ação de atores maliciosos. Isso foi sinalizado no recente banimento, por parte da Agência Nacional de Vigilância Sanitária, da utilização da plataforma Zoom Meeting em seus computadores, medida tomada após a publicização de vulnerabilidades securitivas que viabilizaram o acesso indevido por terceiros a credenciais dos usuários e informações trocadas em reuniões.

• Metodologia e formas de participação desenvolvidas durante o Workshop:
Após uma breve introdução realizada pela moderação a respeito da temática abordada pelo workshop, cada painelista terá cerca de 15 minutos para a apresentação de um tema específico relacionado à seguinte questão que direcionará o workshop: “Qual a importância das políticas de segurança da informação, sobretudo aquelas relacionadas à criptografia, para o teletrabalho e serviços ofertados no âmbito digital?”.
Em seguida, serão reservados, aproximadamente, 25 minutos para perguntas, respostas e interações diversas após a exposição dos palestrantes.

3. Síntese dos debates

• Síntese dos posicionamentos e propostas apresentadas pelos(as) palestrantes e participantes (incluindo as perguntas);

• Identificação de consensos, pontos a aprofundar e dissensos.

Tipo de Manifestação (Posicionamento ou Proposta)	Conteúdo	Consenso ou Dissenso	Pontos a aprofundar
Discutir com o público geral a importância da	- Apresentação de dados sobre a massificação do	Consenso	Dar visibilidade e trazer para discussão

criptografia e da segurança da informação, principalmente dentro de um contexto de pandemia, onde as relações pessoais foram digitalizadas e o teletrabalho foi intensificado passando a ser o “novo normal”	teletrabalho e dados de incidentes de segurança da informação durante a pandemia. - 8,3 milhões de pessoas trabalham remotamente no Brasil (13% da população de trabalhadores do país). - Deste número, a maior porcentagem é de servidores públicos, 357 mil servidores trabalhando remotamente (63% de toda a força de trabalho do governo federal). - O despreparo das instituições e da sociedade civil para enfrentar estes desafios, principalmente devido a falta de recursos imediatos para atender estas novas demandas. - Apresentação de uma pesquisa realizada na Europa onde 51% dos respondentes disseram que seus funcionários não estão adequados ou foram treinados para lidar com riscos de segurança da informação; trazendo outros índices também sobre a insegurança digital dos usuários. Um fator importante é que a pesquisa apontou que 40% dos respondentes afirmou que estão cortando investimentos em cibersegurança, devido a crise econômica. - Os dados ajudam a fundamentar a preocupação com os riscos do salto abrupto ao teletrabalho e com o aumento da vigilância, exemplificados pelo aumento de ataques de phishing e		pública, os desafios que temos para enfrentar em relação a segurança da informação e direitos humanos. - A urgência de se discutir os desafios do teletrabalho já que parece ser um modelo que veio para ficar. - A necessidade de opções diferenciadas das soluções “prontas” apresentadas que tiram do gestor o controle da segurança da informação. - O paradigma da resiliência quanto aos dados: a questão não é “se” os sistemas sofrerão ataque, mas sim “quando” os ataques acontecerão.

	ações de enfraquecimento da criptografia e da privacidade. Estes riscos afetam diretamente direitos fundamentais. - A importância de se desenvolver um arcabouço robusto de segurança da informação (estratégias políticas e princípios) desenvolvendo também uma cultura da segurança, o papel das plataformas e políticas de educação digital.		
Os desafios da implementação do teletrabalho nas Defensorias Públicas. Como defensorar em tempos de exceção.	- Desafios de exercer o papel da Defensoria Pública dentro do Sistema de Justiça num contexto de pandemia, que tem como objetivo defender grupos vulneráveis e a promoção de direitos humanos. - Desafio, neste contexto, de garantir a relação da Defensoria Pública com a população atendida: 1) dificuldade da população em fazer uma adaptação para a versão do atendimento virtual, tanto por dificuldade de acesso à internet quanto pela qualidade dos aparelhos conectados que impedem a instalação dos aplicativos necessários e execuções técnicas (exclusão digital); 2) dificuldade orçamentária que impede uma melhor adaptação para este atendimento virtual, forçando que muitos defensores públicos passassem a usar seus celulares e computadores pessoais para	Consenso	- Preocupação com a possibilidade de realização de plenárias de júri dentro destes ambientes virtuais. - Processos pouco pensados que foram adaptados para o teletrabalho sem nenhuma construção crítica sobre os seus impactos. - Investimentos financeiros pessoais dos funcionários para bancar as necessidades tecnológicas trazidas pelo teletrabalho.

	a execução dos atendimentos; 3) capacitação dos próprios profissionais às novas tecnologias e conceitos de segurança da informação; 4) digitalização dos processos. - Desafio da atuação da Defensoria Pública em juízo: 1) dificuldades das partes em entender e se adaptar às ferramentas onlines, muitas vezes privadas, de realização das audiências; 2) o desafio da explicação e educação sobre estas tecnologias recaírem nos defensores públicos; 3) a necessidade de se garantir a segurança técnica da ferramenta e a segurança das informações trocadas naquele ambiente de videoconferência; 4) garantia de que os direitos fundamentais e deveres das partes envolvidas, sejam assegurados durante as audiências, ex: testemunhos por vontade própria sem influência de terceiros, sigilo das conversas entre réus e defensores, etc; 5) baixa preocupação, por parte do sistema judiciário, em assegurar os direitos fundamentais referente a segurança das informações envolvidas nos processos.		
- Como a pandemia vem afetando o uso do WhatsApp nas relações profissionais no Brasil. - A importância da criptografia de	- Chamadas de voz e vídeo dentro do WhatsApp, durante a pandemia, mais que dobraram. - O pico de troca de mensagem dentro do aplicativo já superou a de 100	Consenso	- A preocupação do WhatsApp em democratização do acesso à contas oficiais e informações oficiais sobre o Covid19.

ponta-a-ponta.	bilhões de mensagens por dia, no mundo. - Pesquisa recente aponta que 94% dos brasileiros usam WhatsApp para se comunicar, e deste público, 64% também usam o WhatsApp para trabalho, principalmente dentro do público jovem entre 16 e 34 anos. Um dos pontos da pesquisa demonstra também o crescimento do acesso ao aplicativo pelas classes mais baixas que passaram a usar a internet também para trabalho. - O WhatsApp passou a ser uma opção para o pequeno e médio empreendedorismo brasileiro durante a pandemia, por permitir a atuação do negócio mesmo durante o distanciamento social. Outra pesquisa mostra um crescimento significativo do aplicativo para realização de compras online. - Enfoque no crescimento do uso do WhatsApp pelos profissionais de saúde durante a pandemia.		- A preocupação da ferramenta em garantir princípios de segurança da informação através da autenticação de dois fatores e também da criptografia de ponta-a-ponta aos seus usuários, principalmente dentro do cenário de pandemia, quando serviços essenciais que lidam com informações sensíveis passam a adotar o WhatsApp como sua principal ferramenta. - O problema da solicitação, por parte do setor de segurança pública, de medidas de enfraquecimento da criptografia, como no caso do bloqueio do WhatsApp no Brasil devido a impossibilidade de cederem informações criptografadas.
- Como se configura o atual arcabouço protetivo da segurança da informação, diante dos desafios impostos pela digitalização acelerada durante a pandemia.	- Aumento em 47% dos incidentes de vazamento de dados durante a pandemia. - Falta de preocupação e investimento, por parte do setor público, à segurança da informação. - Falta do incentivo público a uma educação digital. - Agravamento das situações de falta de segurança digital por parte dos serviços públicos, já que o cenário	Consenso	- Dentro do planejamento de se ter um governo digital até 2022, é necessário se pensar como esta digitalização irá acontecer. - Fortalecimento da técnica da criptografia e de uma criptografia nacional, através do Plano Estratégico

	pré-pandêmico já apontava uma despreocupação com questões de segurança da informação. - Vale lembrar que em 2019 o SUS teve um grande vazamento de dados, incluindo Nome, Nome de mão, CPF e outro, devido ao API que a plataforma usava. No Pernambuco, já este ano, houve o vazamento de dados de estudantes da rede pública e privada, que incluíam fotos e informações de login. - É preciso a consolidação da cultura de proteção de dados no Brasil, que pode surgir agora a partir da efetivação da Lei Geral de proteção de Dados. - O falso entendimento do legislativo de que a criptografia é um artifício que encoberta criminosos. - Estudo do I.Prec sobre os monitoramento dos projetos de lei que atacam a criptografia. - Julgamento do STF sobre a legitimidade do bloqueio de serviços, como o caso do bloqueio do WhatsApp.		Nacional de Segurança Cibernética de 2020, incentivando uma parceria multisetorial. - A contradição de termos o fortalecimento da criptografia no plano estratégico e ao mesmo tempo, um legislativo e um judiciário que ataca a mesma criptografia e busca o seu enfraquecimento.