idn brief

Especial Pandemia

9 de julho de 2020

CIBERSEGURANÇA E CIBERDEFESA EM TEMPOS DE PANDEMIA

Helena Carreiras

Neste IDN brief convidamos diversos especialistas a identificarem os impactos da pandemia nas áreas da cibersegurança e ciberdefesa. Os seus contributos são convergentes e complementares na identificação desses impactos e tocam uma ampla variedade de tópicos: as mudanças nos planos da organização social e profissional, a cibercriminalidade e as suas novas faces, a desinformação, os desafios da capacitação e da literacia digital, a necessária, mas difícil, cooperação internacional, a urgência da aposta na ciber-resiliência. E deixam-nos questões críticas: como poderemos combinar medidas privadas e públicas? De que forma essa articulação implica um novo conceito de segurança pública e segurança nacional? Conseguiremos equilibrar benefícios e custos da transição digital? Fazer coexistir conexão e privacidade? Estaremos preparados para assumir os custos de desenvolver ciber-resiliência?

DIRETORA
Helena Carreiras
COORDENADOR EDITORIAL
Luís Cunha
CENTRO EDITORIAL
António Baranita e Luísa Nunes
PROPRIEDADE, DESIGN GRÁFICO E EDIÇÃO
Instituto da Defesa Nacional
Calçada das Necessidades, 5, 1399-017 Lisboa
Tel +351 211 544 700
idn.publicacoes@defesa.pt
ISSN 2182-5327
Depósito Legal 340906/12

idn Instituto da Defesa Nacional

Cibersegurança e Ciberdefesa em Tempos de Pandemia

Cibersegurança em Tempos de Pandemia

André Barrinha
Professor Associado em Relações Internacionais, Universidade de Bath

Como recentemente salientou Herb Lin[1], a primeira referência ao conceito de "vírus informático", remonta a 1984, num artigo de Fred Cohen. A melhor forma de combater essa nova ameaça era através daquilo a que o autor chamava de "isolacionismo": quanto menos ligados ao mundo estivessem os nossos computadores, menos riscos de infeção correríamos. Aquilo que em 1984 – e, de certa forma, ainda hoje – resultava para a segurança informática, é hoje a principal receita aplicada no combate ao Covid-19. O grande desafio hoje está justamente no cruzamento das duas ameaças: a biológica e a informática. A melhor forma de nos protegermos de ataques cibernéticos é trabalharmos a partir de instituições com arquiteturas de segurança robustas, mas a melhor forma de nos protegermos do vírus é ficando em casa onde usamos os nossos meios informáticos pessoais para uso profissional. O Covid-19 fez com que milhões de pessoas passassem a aceder às redes e servidores das suas empresas e organizações a partir de casa e através de redes com níveis de segurança inferiores. Não é por isso de espantar que tenha havido um aumento generalizado de ataques cibernéticos, com o FBI a dar conta, em abril último, de um crescimento de 300% no número de queixas relativas a ataques informáticos. O mesmo cenário verifica-se um pouco por todo o mundo.

Infelizmente, o Covid-19 serviu também para colocar hospitais e instituições de investigação médicacomo alvos preferenciais de ataques cibernéticos. A própria Organização Mundial de Saúde viu 450 endereços de email e respetivas *passwords* dos seus funcionários divulgados *online* após múltiplos ataques. O problema nesta área – tal como ficou visível com o ataque *WannaCry* de 2017 que impediu o normal funcionamento do serviço nacional de saúde britânico durante um fim-de-semana inteiro – é que instituições hospitalares, pela lógica do seu funcionamento, são avessas a atualizações de *software* e a boas práticas de higiene cibernética: estão sempre abertas, os aparelhos que utilizam estão em constante utilização e são espaços sujeitos a circulação diária de milhares de pessoas, incluindo médicos e funcionários – muitas vezes cansados e sob pressão – com acesso a computadores e servidores.

Quer seja por tentativas de extração de informação por parte de Estados, ou simples extorsão – através de *ransomware* – a indivíduos ou a instituições hospitalares a trabalhar no limite por criminosos que veem na atual situação uma forma de lucro fácil, esta pandemia veio salientar – no que será um dos seus principais legados – a importância da cibersegurança para o funcionamento das nossas sociedades, cada vez mais digitalizadas e agora também descentralizadas. Porque o isolacionismo informático simplesmente não é opção, veio também colocar a nu a absoluta necessidade de cooperação internacional nestas matérias, o que não será fácil num contexto internacional atomizado e sem um fórum permanente de discussão para matérias de cibersegurança.

Nota

[1]Herb Lin, 2020. Cybersecurity Lessons from the Pandemic, or Pandemic Lessons from Cybersecurity. *Lawfare* [em linha], June 2, 12:36 PM. Disponível em https://www.lawfareblog.com/cybersecurity-lessons-pandemic-or-pandemic-lessons-cybersecurity

Resiliência Física *versus* Resiliência Digital

António Gameiro Marques
Diretor-geral do Gabinete Nacional de Segurança

Lino Santos
Coordenador do Centro Nacional de Cibersegurança

A História tem-nos mostrado que momentos como os que estamos a vivenciar são reiteradamente promotores de fraturas com o passado e simultaneamente potenciadores de novas formas de viver, quer no contexto pessoal quer no âmbito da nossa vida em sociedade.
Esta nova "forma de estar" assenta, em grande medida, no reforço da tecnologia como instrumento de mitigação do distanciamento social e do constrangimento na mobilidade a que estamos sujeitos, evidenciando a natureza resiliente do ser humano.
Com efeito, tendencialmente pensamos e desenvolvemos o conceito de resiliência como a tolerância a falhas dos sistemas informáticos que suportam o bom funcionamento da nossa economia e o bem-estar da nossa sociedade.
Neste sentido, e tendo como pano de fundo um eventual *Armagedom* cibernético, foram desenvolvidas políticas, processos e programas de treino para reduzir a dependência e encontrar alternativas à tecnologia (no mundo analógico), de forma a evitar disrupções económicas e, no limite, distúrbios da ordem pública.
Todavia, a crise de saúde pública que vivemos veio chamar a atenção coletiva para a resiliência na lógica da tolerância a falhas do nosso mundo físico, situação que só os visionários anteciparam e para a qual poucos estariam preparados.

Neste contexto, as restrições à atividade económica e o confinamento obrigatório, forçaram o Estado, as empresas e as pessoas a procurar alternativas para prosseguir com a sua missão ou simplesmente socializarem. Desta forma, o digital ganhou maior importância na nossa sociedade. Excetuando o contexto familiar, o digital deixou de ser mais um meio onde agimos e interagimos, para passar a ser o meio onde estamos permanentemente e sem o qual a nossa atividade social e corporativa não se realiza. Alguns indicadores já disponíveis sobre o período entre março e maio deste ano, revelam um crescimento superior a 40% dos volumes de tráfego de voz e dados em Portugal, um aumento de 90% do comércio eletrónico em Itália ou um acréscimo de cerca de 75% na utilização das redes sociais em Espanha. Na mesma medida, o tema da cibersegurança ganhou maior importância na nossa sociedade.
A previsível transição do tradicional ambiente de trabalho para um regime exclusivo ou tendencialmente misto de teletrabalho, com a inevitável diluição da fronteira entre os contextos familiar e profissional, vem criar novos desafios às lideranças e às organizações. Assim sendo, é da maior importância que esta transição tenha por base uma rigorosa avaliação de risco e que sejam feitos os necessários investimentos nas pessoas e na tecnologia, sob risco de as organizações tenderem para alguma desagregação, e dos perigos perpetrados através do ciberespaço terem impactos muito significativos em todo o espectro da sociedade. É por isso fundamental sermos cautelosos e firmes no combate ao deslumbramento que a novidade aporta e pesar, de igual forma, os benefícios e os custos, em todas as suas dimensões, necessários para mitigar os inevitáveis riscos que essa transição comporta.
Importa, ainda, dar nota de que os níveis de ansiedade e de solidão, provocados pela condição de anormalidade decorrente das medidas de combate à pandemia, representam um fator de risco para indivíduos e organizações. Não sendo um fenómeno novo – sempre que um tema capta a atenção da população, ele é usado por diferentes agentes de ameaça para ações de engenharia social –, a narrativa em torno do Covid-19 tem vindo e continuará a alimentar, entre outras, campanhas de furto de identidade, infeção com *malware* e desinformação. Neste contexto, é da maior importância o reforço do espírito crítico e da literacia digital dos nossos cidadãos, dotando-os das capacidades necessárias para "estar" e tirar o devido partido, em segurança, neste ciberespaço.

A Pandemia de COVID-19 e os Ciberataques em Portugal

Daniela Santos
Responsável pelo Programa de Sensibilização e Treino em Cibersegurança, Centro Nacional de Cibersegurança
Investigadora CIES-ISCTE

A pandemia de COVID-19 veio acelerar a tendência de aumento, em número e em sofisticação, dos ciberataques, que temos visto nos últimos anos.
Com a necessidade de distanciamento físico entre as pessoas, as atividades laborais foram repensadas e milhões de trabalhadores, em poucos dias, passaram a desempenhar as suas atividades laborais em regime de teletrabalho.
A forma e a rapidez desta transição foi um sucesso, considerando as

circunstâncias, mas o aumento exponencial do número de denúncias de ciberataques a organizações e cidadãos neste período evidenciou, por um lado, o aproveitamento que os atacantes fizeram desta oportunidade para tentar penetrar nas redes e sistemas das organizações e, por outro, a necessidade de sensibilizar e formar mais os cidadãos para a ciber-higiene e de informar sobre os perigos associados ao uso desprotegido da Internet e outros meios de comunicação *online*.

Como publicado no boletim de maio do Observatório de Cibersegurança, do Centro Nacional de Cibersegurança (CNCS), entre fevereiro e março de 2020, o número de incidentes registados pelo CERT.PT – serviço que coordena a resposta a incidentes de cibersegurança no ciberespaço de interesse nacional – aumentou 84% e, em comparação com o número de incidentes registados em março de 2019, o aumento foi de 176%. Os meses de abril e maio confirmaram esta tendência, com aumentos de 142% e 134%, respetivamente, relativamente ao período homólogo de 2019.

Segundo a mesma fonte, o tipo de incidente reportado com maior aumento neste período de pandemia foi o *phishing*, que aumentou 217% entre fevereiro e março. Os autores destas campanhas de *phishing* aproveitaram o confinamento para simular serviços digitais com maior consumo e fidelização, como os serviços de *homebanking*, conteúdos digitais em *streaming* e lojas *online*.

A pandemia evidenciou também o papel das redes sociais na difusão de desinformação e como meio privilegiado de disseminação de campanhas de *phishing*. Mostrou, de forma muito clara, como os cibercriminosos exploram os receios das pessoas com o intuito de induzir certos comportamentos como, por exemplo, instalar uma aplicação que prometia ver o número de casos e a sua evolução no concelho de residência ou de trabalho, quando na realidade era uma APP maliciosa, COVID-19 *Tracker*, que instalava *ransomware* nos telemóveis.

Esta experiência em alguns casos desencadeou, e noutros acelerou, um processo de alteração da relação com o local de trabalho para muitos trabalhadores. Embora o teletrabalho seja uma prática comum em algumas organizações, ainda são poucas as que o adotam, e esta pandemia demonstrou que, em certos casos, é possível aumentar a produtividade e reduzir custos, tendo sido o mote para algumas entidades, incluindo a Administração Pública, começarem a implementar este modelo, muito usado noutros países em determinados contextos profissionais.

Aliada à falta de informação e de formação dos cidadãos, esta alteração formou um ambiente propício para o aumento do cibercrime. Por esta razão, pode-se dizer que a pandemia de COVID-19 veio destacar a urgência da criação de uma orientação nacional para a educação e formação dos cidadãos nesta área, direcionada para responder à necessidade de informação e de profissionais com determinadas competências em Portugal.

Ciberespaço e Mundo Físico – As Duas Faces da Mesma Moeda

Helder Fialho de Jesus
Capitão-de-Mar-e-Guerra, Chefe do Centro de Ciberdefesa (CCD) do EMGFA

A COVID-19 veio alterar muitos processos na nossa sociedade, nomeadamente no ambiente de trabalho, onde a presença física era o *modus operandi*, os quais são agora mais assentes no ciberespaço. E os atores das atividades maliciosas, que são rápidos na aprendizagem e na adaptação, também se ajustaram. Como exemplos têm-se atividades ligadas à espionagem, visando o roubo de informação sensível e propriedade intelectual, as relacionadas com o cibercrime, explorando as fragilidades sociais para fazer dinheiro e as associadas à utilização de notícias falsas, para confundir a sociedade e levar os governos e órgãos de informação ao erro, visando fins próprios.

Com esta pandemia verificou-se um enorme crescimento de novas formas de utilização social e profissional das tecnologias existentes. No fundo, acelerou-se algo que iria acontecer mais cedo ou mais tarde, com um impacto significativo na nossa sociedade, a qual é cada vez mais em rede, globalizada, e onde os contextos privados, públicos e profissionais se misturam. Neste contexto, identificam-se três áreas que enquadram esta situação, nomeadamente:

• **Organização social e profissional** - o novo coronavírus fez emergir a necessidade de trabalho remoto para a continuidade das operações, bem como, em muitos casos, a utilização de equipamentos pessoais para fins profissionais, situações estas que podem conflituar com uma política de

segurança rigorosa. A ligação entre os cidadãos e o Estado também passou a assentar mais nas plataformas digitais. As situações referidas aumentam a superfície de ataque, permitindo o aproveitamento por terceiros, sejam eles atores estatais ou de outro tipo, para o desenvolvimento de atividades maliciosas.

• **Cibercriminalidade** – relatórios recentes de diversas entidades competentes referem o seu aumento. Esta pandemia obrigou ao confinamento da sociedade originando um crescimento das atividades à distância, entre elas as compras *online*, as crianças passarem mais tempo no computador devido ao encerramento das escolas, etc. A bondade das pessoas também é explorada por esquemas fraudulentos, onde são solicitados contributos financeiros para o desenvolvimento de vacinas para combater a COVID-19, através de hiperligações falsas em SMS, Emails ou em páginas na internet. Tecnicamente falamos de esquemas conhecidos por *phishing*, *ransonware*, *malware* e outras técnicas que abrangem toda a dimensão de utilizadores do ciberespaço.

• **Desinformação** – através de técnicas de exploração do medo, de proliferação de *Fake News* e da difamação de organizações e pessoas credíveis. Como exemplos podem referir-se as **teorias da conspiração**, nomeadamente com a referência a uma ligação entre a COVID-19 e a nova tecnologia 5G, as **dinâmicas geopolíticas**, entre elas as relativas à origem do coronavírus – EUA *versus* China – e a **difamação de organizações e pessoas**, ilustradas com o comportamento de alguns responsáveis mundiais que inicialmente pouca importância deram a este fenómeno e agora, após demora na adoção de medidas, apontam o dedo à Organização Mundial de Saúde (OMS).

Tendo em vista a redução dos efeitos nocivos das perspetivas apresentadas, o papel de alerta para comportamentos pelas entidades com responsabilidade na proteção, segurança e defesa do ciberespaço é fundamental. E assim garantem-se os valores da nossa sociedade.

Ciber-resiliência: uma Nova Atitude para a Segurança no Ciberespaço?

João Barbas
Coronel
Assessor do Instituto da Defesa Nacional

O ex-Diretor do FBI, Robert Muller, mais conhecido pela investigação da eventual influência russa nas eleições presidenciais dos EUA de 2016, afirmou numa conferência: "I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again".

Esta frase poderá ser entendida por alguns, com algum desânimo, que sendo os ciberataques inevitáveis não se justificaria utilizar recursos públicos ou privados em cibersegurança. Este raciocínio, possível mas falacioso, seria equivalente a afirmar que sendo inevitáveis os acidentes de viação, qualquer medida de segurança rodoviária seria despicienda.

Da mesma forma que no mundo real não é possível obviar comportamentos socialmente reprováveis por antecipação através de videntes, como no filme "Minority Report", ou dissuasão pela omnipresença das Forças e Serviços de Segurança, no ciberespaço estes também não são evitáveis. Que fazer então? Aceitar a inevitabilidade das ameaças e dos ataques?

A resposta a esta questão poderá estar numa palavra muito utilizada em tempos de pandemia: Resiliência. Dizem-nos, ou julgamos saber, que a progressão do COVID-19 à escala global é uma inevitabilidade, desejavelmente de forma controlada e que, no futuro, as nossas sociedades, sendo capazes de limitar e resistir à propagação desta ameaça invisível, serão mais resilientes. O que é então resiliência? E como a procurar alcançar no mundo virtual?

Resiliência é a capacidade de antecipar ou resistir a um acontecimento e retornar a um estado normal num período de tempo considerado aceitável. Por sua vez, ciber-resiliência é capacidade de uma organização "preparar, responder e recuperar" em caso de ciberataque. Uma organização ciber-resiliente deverá ser capaz de se defender desses ataques, limitar o seu impacto e assegurar a continuidade do seu funcionamento após eventuais violações.

A importância da Ciber-resiliência foi reconhecida em diversos relatórios do *World Economic Forum* e em orientações para a resiliência cibernética de instituições financeiras. Estas orientações descrevem cinco categorias de gestão de risco primárias – governação; identificação; proteção; deteção e resposta e recuperação – e três componentes fundamentais – testes; consciência situacional; aprendizagem e evolução. Para alcançar a desejada resiliência é proposta uma abordagem integrada e sinergias nos investimentos associados.

Agora, mãos à obra!

Covid-19 e Cibersegurança: o que Ficámos a Saber sobre as Nossas Decisões?

João Confraria
Universidade Católica Portuguesa

Uma pandemia como a atual era um risco conhecido. O que se passou mostra que nas decisões públicas e privadas não foram considerados todos os riscos existentes.
Na área da saúde, as decisões dos últimos anos estiveram tão alheias a isto que um dos objetivos do confinamento (em todo o lado) foi arranjar tempo para construir capacidade de resposta que não existia. É fácil atribuir isto à inércia do Estado, ou à incompetência deste ou daquela. No entanto, é necessário perguntar: há três ou quatro anos a sociedade aceitaria os custos adicionais na saúde e na segurança social para construir capacidade de resposta a riscos deste tipo? E sabendo o que se passou, aceitamos agora custos adicionais para nos protegermos de riscos futuros?
O processo de decisão do setor privado não esteve muito melhor. Como muitas empresas atuam em concorrência, situação desejável, pode não ser vantajoso para nenhuma delas tomar decisões para se protegerem de riscos como os de uma pandemia, aumentando os seus custos, se as outras não os tomarem também. Além disto, quem previu que não valia a pena esforçar-se muito, porque em caso de tragédia os custos acabariam por ser socializados, não falhou por muito. Isto remete-nos para a criação de regras, nacionais e internacionais, que levem as empresas a fazer os investimentos adequados nos sítios adequados. Aqui, a posição de referência que a União Europeia tem conseguido criar na regulamentação, com a proteção de dados pessoais entre os mais recentes, será útil?
Nalguns setores, boas redes de comunicações permitiram manter um nível razoável de atividade económica, com o comércio eletrónico e o trabalho à distância. Isto não aconteceu noutras pandemias do passado e foi bom para muita gente. Mas mostrou que a falta de cobertura total da população por redes de alta velocidade ou, existindo cobertura, a falta de acesso seguro à internet por motivos económicos ou de iliteracia digital, tem consequências trágicas para muita gente, a começar por professores e alunos em todos os graus de ensino. Não deveria ser difícil conseguir a cobertura total da população, combinando com proporcionalidade medidas políticas e de regulação. Ser fácil não quer dizer que se faça, infelizmente.
Promover a segurança no acesso e uso da internet é mais difícil. O aumento do número de incidentes imputáveis à pandemia, descrito nos boletins do Centro Nacional de Cibersegurança, criou mais dificuldades. Resolvê-las envolve a combinação de medidas privadas, de cada um, com um sistema de segurança público. É um novo conceito de segurança pública e de segurança nacional que se desenvolve.
Finalmente, impõe-se considerar a situação inversa. Estamos preparados para uma pandemia em que o vírus não é biológico, mas digital, com uma capacidade de reprodução muito maior? Isto é, estamos preparados para suportar os custos que protejam a vida económica e social do confinamento digital que nesse caso seja necessário?

Covid-19 e Desafios para a Cibersegurança num Tempo pós-Pandemia

Luis Borges Gouveia
Professor Catedrático, Universidade Fernando Pessoa

Vivemos tempos de mudança. Verdadeiramente, muito do que pautava as condições de mudança efetiva numa eventual nova ordem, estava já em andamento desde o início do presente século. São várias as caraterísticas novas: a intensidade de circulação de pessoas, de bens e fluxos financeiros e, mais expressivo, de informação. A crescente mobilidade de pessoas e sua circulação quer em contexto de turismo ou de formação em contexto de educação superior, fomenta a existência de um mercado crescente de competências humanas, disponíveis de contratar, a uma escala global, independentemente da sua origem ou localização, mas cognitivamente ligadas.
Mas qual a relação com a cibersegurança? É que toda esta dinâmica é assente em infraestruturas de comunicação de dados e de redes de informação. Melhor ainda, são objeto de agregação de valor, por via de plataformas digitais. Possuir sistemas de informação competentes apenas alcança o comando e controlo. A oferta de valor e a capacidade de projeção e de adaptação que o digital patrocina é essencialmente resultado do maior ou menor grau de controlo e capacidade de capturar utilizadores para plataformas digitais que oferecem serviços em troca da produção de

dados e inteligência – talvez o valor acrescentado real deste tipo de investimentos.
Como resultado do digital e sem as barreiras físicas associadas com a contraparte analógica, que tradicionalmente nos proporcionou a organização de espaços em territórios, estes novos territórios digitais são transversais. Ora, as redes apresentam um potencial que, para se concretizar têm de ser abertas e, logo, expostas às vulnerabilidades e à complexidade de acomodar as competências dos seus potenciais utilizadores.
Este cenário existia a janeiro de 2020 e a pandemia da doença Covid-19 teve o impacto de proporcionar uma visão de Raio-X a um contexto emergente de transformação (digital) que se está a desenhar (amplificando riscos e vulnerabilidades). Verdadeiramente, assistimos à aceleração de um processo que seria gradual, também pelo combate dos atores mais tradicionais, ainda na posse de argumento, capacidades e solidez, que, entretanto, se esfumou.
Entre as mudanças contam-se as transições rápidas (e desordenadas) para o ensino de emergência e em casa e para o teletrabalho (em confinamento). Por via de uma transição abrupta, muitos dos sistemas de informação tiveram o seu comportamento adaptado e foi necessário considerar ferramentas novas ou novas funcionalidades de ferramentas digitais. Tal criou um crescimento significativo associado com a literacia digital. No entanto, muitos dos sistemas de informação foram em limite descaracterizados ou incorporam uma maior complexidade. Em resultado, a exposição e o risco associado com o uso de redes, acesso e segurança da informação, tornou-se bem mais desafiante e agora, definitivamente, uma questão sistémica, de natureza coletiva e a exigir monitorização constante – paradoxalmente, muito como parece ser a natureza do corona vírus associado a este novo desafio à escala global.
Temos assim, um contexto que multiplica complexidades e cruza as questões de cibersegurança, a uma escala que, apesar de tudo, é ainda maior de que a que vivíamos. As plataformas digitais, as ferramentas utilizadas, as questões da segurança da informação e a proteção de valor, bem como a sua partilha, tem de constituir um jogo em modo de redes abertas. As questões de literacia e das competências digitais constituem aspetos relevantes para assegurar (e exercer) soberania.
A procura de perfis mais digitais, de novos comportamentos associados com a transformação digital, exigem recursos humanos devidamente preparados e o seu emprego (local ou global) tem, para o território físico, importância capital. Preparar capacidades de cibersegurança, assegurando a sua prática e garantir um ecossistema digital seguro e fiável, populado por unidades de carbono que sejam capazes de o compreender, é crítico. Esta pode ser uma ambição nacional, de segurança e defesa e de partilha de valores alicerçados em competências suficientes de cibersegurança, que proporcionem um espaço de valor, muito atrativo para a captura de investimento global, no tempo pós pandemia que se vai seguir.

A Face Digital da Pandemia COVID-19: Cibersegurança, Ciberdefesa e Resiliência Nacional

Paulo Fernando Viegas Nunes
Coronel Tm (Eng)
Docente do Instituto Universitário Militar e da Academia Militar

A pandemia COVID-19 expôs as fragilidades das modernas sociedades para lidar com situações de exceção, emergência ou crise nacional. Esta situação sanitária atípica, veio também provar a elevada dependência das modernas sociedades relativamente às tecnologias da informação, à internet e ao ciberespaço.
Não só em Portugal, mas também à escala mundial, a transformação digital sofreu uma forte aceleração, um verdadeiro salto qualitativo, estimulando a inovação tecnológica e reforçando a resiliência nacional. Apesar de social e fisicamente distantes, o futuro das modernas sociedades perspetiva-se hoje em rede e mais interligado do que nunca. Facilitando a construção de comunidades virtuais, de forma quase imediata e ajustada às necessidades emergentes das organizações, o ciberespaço funcionou como um elemento conectivo da sociedade, permitindo ultrapassar distâncias físicas, constituindo-se como um verdadeiro “centro de gravidade funcional”.
Ao longo desta crise, as operadoras e os fornecedores de acesso à internet adaptaram os níveis de serviço, reforçando as suas infraestruturas. Serviços públicos, escolas e empresas ajustaram-se rapidamente à “nova normalidade”, adotando práticas de teletrabalho e convertendo os

tradicionais processos de interação em videochamadas, utilização de redes sociais e programas de *chat*.
A repercussão mundial desta crise originou uma procura constante de informação. Os comportamentos de risco na internet aumentaram com uma maior utilização e tempo passado *online*, facilitando a disseminação de *software* malicioso e *ransomware.*
Em tempos de pandemia, de forma a limitar as taxas de infeção digital, impõe-se uma alteração do comportamento individual, ajudando a manter a cibersegurança coletiva.
Reforçando tendências anteriores, conforme identificado num estudo recente do Instituto Universitário Militar relativo ao impacto estratégico da pandemia COVID-19, registaram-se ciberataques a centros de conhecimento e tecnologias de ponta. Foram igualmente identificadas campanhas de desinformação lançadas por Estados que procuraram, através dos media e das redes sociais, manipular grupos e induzir conflitos sociais noutros países, através de narrativas disruptivas (*fake news*), alargando assim a sua esfera de influência. Este tipo de atividades, teve também por alvo organizações internacionais como a Organização do Tratado do Atlântico Norte e a União Europeia.
Apesar de durante a pandemia COVID-19 não terem sido assinalados ataques de grande capacidade disruptiva e/ou destrutiva, o grande volume de ataques cibernéticos veio provar a necessidade de robustecer as capacidades de cibersegurança e ciberdefesa do País.
Após o início deste surto, os ciberataques aumentaram em número e impacto, afetando indivíduos, organizações e Estados, podendo, numa situação limite, vir a comprometer as infraestruturas críticas nacionais e pôr em causa a resiliência do Estado. Num quadro desta natureza, configurando também esta uma situação de exceção, as Forças Armadas podem vir a ser chamadas a intervir no âmbito da cibersegurança nacional, nomeadamente, para assegurar a defesa digital (ciberdefesa) do Estado.
No pós-COVID-19, os alicerces da agenda digital de Portugal, que se perspetiva potenciadora do desenvolvimento estrutural e da competitividade nacional, só poderão materializar-se através de uma utilização mais aberta, livre e segura do ciberespaço. Para que estes desafios estratégicos sejam atingidos com sucesso, torna-se necessário reforçar o investimento na literacia digital, na sensibilização para uma utilização mais segura das novas tecnologias e no fortalecimento da capacidade de cibersegurança e ciberdefesa nacional.

A Excecionalidade do Covid-19 e a Redefinição da Privacidade

Sofia José Santos
Professora Auxiliar e Investigadora
Faculdade de Economia e Centro de Estudos Sociais, Universidade de Coimbra

Perante a pandemia COVID-19, vários Estados têm recorrido ao uso de aplicações informáticas para ajudar a conter a doença nas suas fronteiras. Ainda que com nomes, possibilidades e contornos distintos, estas aplicações assumem como denominador comum as funcionalidades de permitir potenciar o distanciamento social entre utilizadores/as, através do mapeamento cumulativo e cruzado de dados de geo-localização, rastreando simultaneamente os contactos estabelecidos e recolhendo informação sobre a saúde de quem as utiliza. China, Austrália, México e Coreia do Sul foram alguns dos primeiros países a implementar estas medidas de vigilância.
Alinhada com a conhecida ideia – aplicada a cenários de *early-warning* – de que conexão é proteção, o leque de escolhas que se abre em relação a estas aplicações no atual contexto COVID-19 é não raras vezes apresentado como uma troca cirúrgica e utilitarista entre saúde e privacidade. Porém, apesar do raciocínio linear com que nos apresentam a equação, a relação entre conexão e proteção, particularmente na área da cibersegurança, é sempre uma relação de termos calibráveis. Isto quer dizer que o que significa e implica conexão bem como a ameaça e o referente de segurança que definem os termos da proteção dependem de cada momento, contexto e, sobretudo, da subjetividade e lugar de enunciação do ator em causa. No caso concreto das aplicações para rastrear a COVID-19, a conexão implica o debate sobre o acesso sem discriminação à internet, mas o significado de proteção oscila entre a securitização da privacidade e a securitização da saúde, sendo a equação habitualmente desenhada numa lógica dicotómica ou mutuamente excludente.
Esta exigência de hierarquização quase impossível tem dividido as opiniões - em alguns casos de forma profunda.
Do lado da contestação, o primado da privacidade tem sido a principal bandeira. Porém, mesmo em movimentos contra-hegemónicos, a privacidade tem sido tendencialmente representada como se de um conceito homogéneo se tratasse. Ou seja, como se a garantia da privacidade e a vulnerabilidade face à ausência dessa garantia fosse distribuído e sentido nas sociedades de forma igual e universal. Se o ambiente *online* e o *offline* não são dissociáveis e se alimentam

reciprocamente, o que se passa na ciberesfera não deixa, pois, de refletir e privilegiar os entendimentos hegemónicos sobre quem é uma ameaça e quem deve ser protegido. Daí que tanto a cibersegurança como a tecnologia que a garante e a desafia sejam sempre subjetivas, relacionais, contextuais e políticas.

No contexto COVID-19, muito pouco se tem debatido sobre que dados são relevantes, como é feita a recolha desses dados, qual a engenharia algorítmica em que recolha e análise assentam e quais os impactos societais dessas escolhas. Sem transparência e debate, não só as aplicações para combater o COVID-19 tendem e podem reforçar sistemas de discriminação e desigualdade, como a responsabilidade sobre os eventuais danos causados por essas arquiteturas e metodologias invisibilizadas não pode ser apurada.

Este é um dos principais desafios de equilíbrio entre cibersegurança e direitos humanos que se coloca aos decisores políticos no atual contexto de pandemia. Parafraseando Jathan Sadowski "exercer o poder não se resume a alcançar resultados, mas sim a tomar as rédeas dos processos e dos parâmetros da decisão". Do lado da opinião pública, é também importante refletir e atuar sobre os desafios que as questões da privacidade nos levantam. Nesta matéria, várias têm sido as iniciativas para uma discussão alargada e definição de políticas públicas informadas sobre privacidade na luta contra o COVID-19. O futuro pós-COVID-19 será em grande medida desenhado agora – pelas medidas adotadas pelos Estados e pelas discussões que trouxermos para cima da mesa.

COVID-19 e Cibersegurança: a Mente Humana como Infraestrutura Crítica

Sofia Martins Geraldes
Investigadora integrada e doutoranda, Instituto Universitário de Lisboa (ISCTE-IUL), Centro de Estudos Internacionais

A atual crise pandémica gerada pela COVID-19 tem exigido medidas de distanciamento e isolamento físico, implicando uma maior dependência do ciberespaço para vivências pessoais, sociais, profissionais, escolares, entre outras. Consequentemente, atores maliciosos encontram no ciberespaço terreno fértil para explorar vulnerabilidades resultantes do medo, da ansiedade, da pesquisa constante de informação e de produtos – nomeadamente equipamentos de proteção individual e produtos farmacêuticos – e da ausência de informação consensual entre especialistas.

O ciberespaço nem sempre foi considerado uma matéria de segurança. Porém, o caráter em rede dos sistemas informáticos, que controlam objetos como comboios e transformadores elétricos, e a crescente dependência digital dos Estados e das sociedades modernas para a realização de diversos processos têm gerado uma percepção de vulnerabilidade e contribuído para a securitização deste espaço, traduzindo-se na adoção de políticas de cibersegurança. A cibersegurança de uma forma simplista pressupõe a segurança das três camadas subjacentes ao ciberespaço – física, lógica e social. Contudo, governos e organizações internacionais têm centrado a sua atenção na proteção das camadas física e lógica, marginalizando a camada social.

Porém, a pandemia COVID-19 vem confirmar, de entre várias dinâmicas, a necessidade de um maior comprometimento com a camada social, que se tem apresentado como a mais vulnerável.

Neste cenário, tem-se assistido a uma série de ciberataques, sendo a engenharia social o mais comum, em que o atacante manipula o alvo para obter informação sensível.

Em Portugal, segundo dados do Centro Nacional de Cibersegurança, têm-se observado campanhas de *phishing*, nas quais atores maliciosos se apropriam da legitimidade de entidades oficiais como a Organização Mundial de Saúde e centros de investigação e laboratórios do setor da saúde para disseminar conteúdos associados à pandemia, com ficheiros orientados para a captação de dados pessoais das vítimas ou para a infeção dos seus dispositivos com *malware*.

Adicionalmente, a pandemia veio também amplificar o debate subjacente à desinformação *online*, tanto na política interna como internacional. Por um lado, tem-se assistido à disseminação de campanhas de desinformação por Estados e atores políticos sobre as origens e a propagação do vírus, contribuindo para situações de tensão internacional. Por outro lado, a atual crise tem sido acompanhada por uma explosão de informação, classificada pelo Diretor-Geral da Organização Mundial da Saúde como *infodemic*.

Neste contexto, é particularmente preocupante o impacto das campanhas de desinformação e das teorias da conspiração na vida real e o seu custo na vida humana.

No que respeita às campanhas de desinformação, a disseminação de mensagens manipuladas sobre a pandemia, nomeadamente sobre formas de tratamento com cloroquina

ou álcool, já contribuiu para situações de intoxicação e envenenamento. Veja-se também as teorias da conspiração sobre a infraestrutura 5G, a qual se diz ser responsável pela propagação do vírus, contribuindo para que no Reino Unido mais de 70 postes de telecomunicações tenham sido vandalizados e levando mesmo à perseguição de alguns engenheiros. Neste sentido, a pandemia veio amplificar diversas dinâmicas subjacentes ao ciberespaço, havendo a necessidade de um maior comprometimento para com a camada social e o reconhecimento da mente humana como infraestrutura crítica.