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