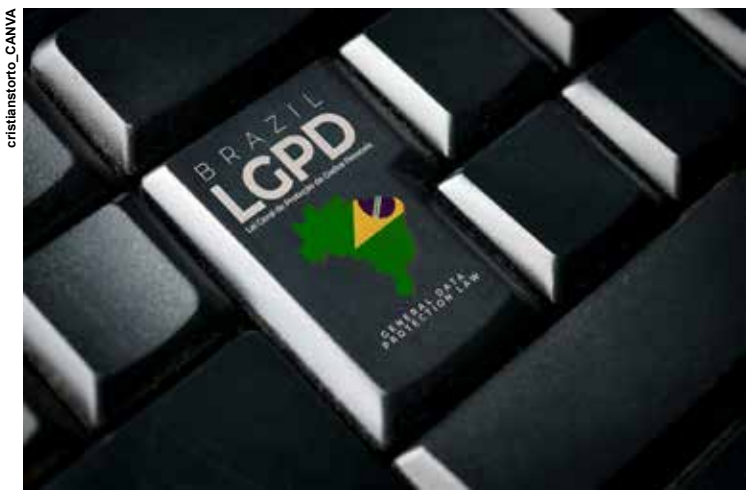
Disparo em massa nas eleições: especialistas alertam para risco de saturação de canais e violação da LGPD

Medida em avaliação no Senado libera disparo automático e inclui um orçamento de quase R$ 5 bilhões para campanhas digitais

A aprovação, pela Câmara dos Deputados, do projeto que autoriza o disparo em massa de mensagens por candidatos durante as eleições, agora em análise no Senado, reacende discussões sobre os impactos da tecnologia na disputa eleitoral e os limites da comunicação digital entre campanhas e eleitores.



cristianstorto_CANVA

A proposta inclui um orçamento de quase R$ 5 bilhões para campanhas, além de mais de R$ 1 bilhão do fundo partidário para despesas permanentes, que poderão ser destinados a disparos via plataformas como WhatsApp, Telegram, SMS e outros serviços semelhantes, acompanhando a migração crescente das campanhas para o ambiente digital. Em contrapartida, especialistas alertam para o risco de aumento do spam eleitoral, da saturação dos usuários e da dificuldade de fiscalização sobre o volume e a origem dos conteúdos disseminados.

"É um tema que exige equilíbrio. De um lado, existe o legítimo interesse dos candidatos em ampliar os canais de comunicação com os eleitores. De outro, é fundamental garantir a privacidade dos cidadãos, a transparência sobre o uso de seus dados e, principalmente, garantir que a ação não tenha um impacto negativo sobre a integridade desse ecossistema digital", afirma Guilherme Rocha, fundador e CEO da HelenaCRM.

Para o especialista, a autorização para disparos em massa por meio de sistemas automatizados, ainda que restrita a contatos previamente cadastrados, traz uma questão central para o debate: qual a origem desses dados e em que medida houve consentimento efetivo dos eleitores para o recebimento desse tipo de comunicação?

"Em um ambiente onde bases de dados circulam com facilidade, muitas vezes sem total transparência sobre sua coleta e compartilhamento, surge o questionamento sobre quantos desses contatos foram fornecidos voluntariamente pelos usuários e quantos apenas integram mailings adquiridos ou compartilhados ao longo do tempo. Abre-se uma brecha para questionamentos sobre consentimento e uso indevido de informações pessoais, um tema que dialoga diretamente com a Lei Geral de Proteção de Dados (LGPD)".

Além disso, de acordo com Guilherme Rocha, mensagens em massa só tendem a produzir resultados positivos quando chegam ao público correto e são recebidas de forma consentida. Quando o envio ocorre de maneira aleatória ou sem autorização do destinatário, o efeito pode ser justamente o oposto, gerando rejeição, desgaste da imagem do candidato e percepção negativa por parte do eleitor.

Entretanto, a principal preocupação está nos impactos que a medida pode gerar sobre os mecanismos que hoje ajudam a preservar a qualidade da comunicação digital. Plataformas como o WhatsApp desenvolveram, ao longo dos anos, sistemas de autorregulação baseados no comportamento dos usuários, incluindo bloqueios, denúncias e até o banimento de contas que realizam envios abusivos. Embora pouco perceptíveis para quem utiliza o aplicativo no dia a dia, esses recursos são fundamentais para manter o ambiente funcional, seguro e confiável.

"Quando uma legislação passa a limitar ou flexibilizar esses mecanismos, cria-se um descompasso entre as regras da plataforma e a experiência do usuário. Mesmo que de forma temporária, isso pode abrir espaço para o aumento do spam e comprometer a qualidade das interações dentro do canal", explica Rocha.

O executivo cita o caso das ligações telefônicas, hoje amplamente ignoradas pela população devido ao excesso de abordagens abusivas, muitas delas legítimas, mas indistinguíveis de tentativas de golpe. "Você inutiliza um canal riquíssimo por conta do excesso. As pessoas deixam de atender porque partem do princípio de que aquilo é indesejado. Isso aconteceu com a telefonia, aconteceu com o e-mail e pode acontecer com aplicativos de mensagem".

Do ponto de vista estratégico, não há dúvida de que o disparo em massa pode aumentar o alcance das campanhas e reduzir custos operacionais. Em um ambiente competitivo e altamente fragmentado, falar diretamente com o eleitor, no dispositivo mais pessoal que ele possui, o celular, é uma vantagem poderosa. "Não é só sobre essa iniciativa, é sobre o que vem depois. A gente pode transformar um ambiente que hoje é saudável em um ambiente saturado. Ou seja, essa eficiência pode ter um custo de longo prazo: desengajamento, bloqueios em massa e perda de credibilidade do canal. Um ativo valioso, a comunicação direta, pode ser rapidamente desgastado", enfatiza o executivo.

"A campanha eleitoral de 2026 pode, assim, marcar não apenas uma disputa nas urnas, mas também um novo capítulo na forma como os brasileiros se relacionam com a informação que chega, todos os dias, na palma da mão", finaliza (https://helenacrm.com/).

A próxima grande crise de cibersegurança pode nascer dentro das empresas

Douglas Barbosa (*)

Existe uma mudança acontecendo dentro das empresas que pouca gente percebeu completamente, mas que deve redefinir os próximos anos da cibersegurança corporativa: o fim da lógica tradicional de proteção. Durante décadas, as companhias acreditaram que segurança significava proteger "os muros" da organização. Firewalls, antivírus, VPNs e barreiras de rede funcionavam como grandes portões digitais. A lógica era simples: proteger o que estava dentro e impedir a entrada de invasores.

Anos depois, o conceito de Zero Trust consolidou essa mudança ao defender que a confiança não deve ser concedida automaticamente com base na localização de rede, no dispositivo ou na suposta presença "dentro" do ambiente corporativo.

O problema é que o mundo corporativo deixou de existir em um único ambiente há muito tempo. Hoje, funcionários trabalham remotamente, sistemas rodam em nuvem, aplicações conversam entre si por APIs e inteligências artificiais já começam a executar tarefas de maneira autônoma. Na prática, as empresas se tornaram ambientes digitais completamente distribuídos. E quando não existe mais um perímetro claro, a pergunta inevitável é: o que precisa ser protegido primeiro? E a resposta é a identidade.

É por isso que o conceito de Identity-First vem ganhando força no mercado de cibersegurança. Em termos simples, significa colocar a identidade digital no centro da estratégia de proteção da empresa. Não apenas a identidade das pessoas, mas também de sistemas, automações, aplicações, robôs e agentes de IA que acessam ambientes corporativos diariamente.

O problema é que muita gente ainda enxerga identidade como algo estritamente operacional: login, senha e permissões de acesso, e esse é um dos maiores erros das organizações atualmente. Hoje, a identidade virou a principal porta de entrada dos ataques cibernéticos. Os criminosos perceberam que invadir sistemas complexos e com muitas proteções, costuma ser mais difícil do que explorar credenciais válidas, permissões excessivas ou acessos esquecidos dentro das empresas. Em vez de "arrombar a porta", eles simplesmente entram utilizando a chave, ou seja, identidades comprometidas.

Dados da Microsoft Security apontam que boa parte dos ataques modernos envolve comprometimento de identidade, e isso muda completamente a conversa sobre cibersegurança. O risco já não está apenas em softwares vulneráveis ou falhas de infraestrutura. Ele está na falta de controle sobre quem, ou o que, possui acesso aos ambientes corporativos.

Vejo que muitas empresas ainda não compreenderam a dimensão dessa mudança e que grande parte das organizações continua investindo milhões em ferramentas de proteção de rede enquanto mantém um ecossistema caótico de acessos, privilégios acumulados e identidades sem governança. É como instalar portas blindadas em uma casa onde centenas de cópias da chave circulam sem qualquer controle.

E esse cenário está se agravando rapidamente por causa da inteligência artificial. A ascensão das IAs corporativas criou uma nova camada de complexidade para a cibersegurança. Isso porque os ambientes digitais passaram a incluir identidades não-humanas como contas de sistemas, automações, APIs, bots e agentes autônomos que também acessam informações críticas e executam ações dentro das empresas.

O problema é que essas identidades crescem em velocidade muito maior do que a capacidade de governança das organizações. Segundo dados da SailPoint, já existe uma proporção estimada de 45 identidades de máquina para cada identidade humana em ambientes corporativos. E aqui existe um ponto que considero extremamente preocupante: muitas dessas identidades simplesmente não possuem um responsável claro. São acessos criados para integrações, automações ou projetos temporários que continuam ativos indefinidamente, sem revisão de privilégios, sem monitoramento contínuo e, muitas vezes, sem sequer alguém saber exatamente para que ainda servem.

Esse talvez seja o novo grande ponto cego da cibersegurança moderna. A discussão sobre Identity-First não é uma tendência passageira de mercado ou discurso técnico e sim uma necessidade operacional urgente, porque, em um ambiente digitalizado, identidade virou infraestrutura crítica e prioridade de governança corporativa. Se uma identidade comprometida - humana ou não - consegue acessar sistemas financeiros, dados estratégicos ou ambientes sensíveis, o impacto deixa de ser um incidente de TI e passa a ser uma crise operacional, financeira e reputacional.

E existe outro ponto que entendo ser crucial destacar: o mercado ainda fala muito sobre ataques externos, mas pouco sobre desorganização interna. Em muitos casos, as próprias empresas criam ambientes inseguros sem perceber. A pressa por inovação, adoção acelerada de nuvem, integrações rápidas e projetos de IA faz com que acessos sejam concedidos continuamente sem uma estratégia sólida de governança. A superfície de ataque cresce silenciosamente todos os dias.

Por isso, o próximo nível de maturidade em cibersegurança será definido não por quem bloqueia mais ameaças na entrada, mas sim pela capacidade das empresas de entenderem, controlarem e governarem identidades digitais de forma contínua. Isso significa saber exatamente quem possui acesso, por qual motivo, até quando aquele acesso faz sentido e qual risco aquela identidade representa para o negócio.

A grande mudança do mercado é que a cibersegurança passou a ser uma questão de confiança digital e, nesse novo cenário, proteger identidades será cada vez mais equivalente a proteger a resiliência e continuidade do próprio negócio.

(*) Business Development Manager da Sec4U e especialista em temas relacionados à identidade digital, governança de acessos e segurança corporativa.

C-Level unido, empresa forte: o desafio da liderança colaborativa

Ricardo Haag (*)

Toda empresa fala sobre colaboração entre os times, mas poucas conseguem aplicá-la de forma efetiva nos níveis mais altos da organização. Mesmo que tenham os melhores talentos do mercado em sua alta liderança, ainda assim, é muito comum que enfrentem dificuldades para crescer de forma sustentável - o que vem dependendo cada vez menos do desempenho individual dos executivos, e mais da capacidade do C-Level de atuar de forma integrada, compartilhando objetivos, responsabilidades e decisões em prol de um propósito maior comum.

Em um ambiente de negócios cada vez mais complexo, quando cada executivo atua em função de suas próprias metas, prioridades ou interesses, a organização perde velocidade, eficiência e competitividade. Não há espaço para lideranças que operam de forma isolada, afinal, desafios complexos exigem respostas construídas coletivamente, e não soluções fragmentadas com base nas visões de cada um.

Um exemplo clássico dessa lógica está no histórico da seleção brasileira masculina de vôlei comandada por Bernardinho. Ao longo dos anos, ele liderou equipes repletas de atletas talentosos, muitos deles considerados os melhores do mundo em suas posições. Ainda assim, o diferencial não estava apenas na qualidade individual de cada jogador, mas na capacidade de todos colocarem um objetivo coletivo acima de seus interesses pessoais: vencer como equipe.

No mundo corporativo, o princípio é o mesmo. Quando o C-Level deixa que metas individuais prevaleçam sobre os objetivos estratégicos da organização como um todo, o resultado é a perda de alinhamento, a fragmentação das decisões e o enfraquecimento dos projetos. Afinal, assim como no esporte, nenhuma empresa conquista resultados excelentes quando cada um joga para si, mas sim quando todos trabalham para ganhar juntos.

Uma pesquisa global da plataforma Mural, divulgada em 2025, comprova isso: apesar de 85% dos profissionais afirmarem que suas equipes colaboram bem, os mesmos admitem existir desalinhamentos frequentes nas metas e prioridades. Além disso, cerca de 90% afirmaram que a falta de colaboração impacta a retenção de clientes, conversões e lançamentos de produtos.

O grande mérito de um bom gestor não é só atrair boas pessoas, mas engajá-las de forma que remem no mesmo sentido. Garantir o comprometimento do C-Level com a mesma visão e que concordem com o caminho a ser seguido não é algo simples, mas fundamental para assegurar a prosperidade corporativa – ao mesmo tempo que, no menor sinal de falta de harmonia entre esses pontos, cabe ao gestor trocar esses executivos, ou revisar o que é esperado pela empresa e por cada um ali dentro.

Não há como ter a utopia de que divergências nunca acontecerão, especialmente quando falamos de executivos experientes, com visões fortes, histórico de resultados e, naturalmente, doses de ego e vaidade que fazem parte do ser humano. Por isso, cabe ao líder monitorar, constantemente, esses sinais que possam indicar um desalinhamento mais profundo, como a falta de boa vontade para colaborar, a redução da participação nas discussões, a ausência de energia para enfrentar desafios coletivos, ou comportamentos sutis como olhares de reprovação e resistência às decisões do grupo.

O caminho é promover conversas abertas, transparentes e francas para compreender o que está por trás daquela atitude e, principalmente, encontrar formas de resgatar o comprometimento com o objetivo comum, antes que os interesses individuais passem a comprometer o desempenho de toda a organização.

No final, criar um C-Level que jogue junto não é sobre eliminar diferenças, mas sobre construir alinhamento em torno de um propósito maior do que qualquer agenda individual. Empresas fortes são aquelas que conseguem transformar talentos distintos em um time coeso, capaz de debater, discordar e até mesmo confrontar ideias sem perder de vista o objetivo maior em comum. Em um mercado cada vez mais complexo e dinâmico, a vantagem competitiva não está apenas na qualidade dos executivos que ocupam o board, mas na capacidade de fazer com que atuem como uma verdadeira equipe.

(*) Headhunter e sócio da Wide Executive Search, boutique de recrutamento executivo focado em posições de alta e média gestão.