



Ética e Integridade



Denise Debiasi



Proteger crianças é uma responsabilidade coletiva



A criação de um canal específico pela ANPD para receber denúncias relacionadas ao descumprimento do Estatuto Digital da Criança e do Adolescente representa mais do que uma nova ferramenta de fiscalização (https://www.gov.br/anpd/pt-br/assuntos/eca-digital/denuncias-eca-digital). Naminha visão, trata-se de um importante sinal de amadurecimento da sociedade diante de um desafio que cresce na mesma velocidade da transformação digital: como proteger crianças e adolescentes em ambientes cada vez mais conectados.

Durante muito tempo, a discussão sobre segurança infantil na internet esteve concentrada nas famílias e nas escolas. Embora esses atores continuem tendo papel fundamental, a realidade demonstra que a responsabilidade precisa ser compartilhada. Plataformas digitais, desenvolvedores de aplicativos, empresas de tecnologia, anunciantes e órgãos reguladores também possuem obrigações relevantes na construção de um ambiente digital seguro.

A iniciativa da ANPD surge em um contexto no qual crianças e adolescentes passaram a conviver diariamente com redes sociais, jogos online, plataformas de vídeo e aplicativos de comunicação. Muitos desses ambientes foram originalmente concebidos para usuários adultos e, apenas posteriormente, precisaram adaptar seus mecanismos de proteção para públicos mais vulneráveis.

Entre os exemplos de irregularidades que podem ser denunciadas estão a ausência de mecanismos adequados de verificação de idade, falhas em controles parentais, coleta excessiva de dados pessoais, práticas que estimulam o uso compulsivo e configurações inadequadas de privacidade. Ao observar essa lista, fica evidente que a proteção da infância digital não depende apenas de impedir conteúdos ilícitos. Ela também envolve a forma como produtos e serviços são concebidos.

Esse é um ponto que considero especialmente relevante. Quando falamos em ética corporativa, muitas vezes pensamos em corrupção, conflitos de interesse ou fraudes. No entanto, a ética também está presente nas decisões de design, nos algoritmos, nas estratégias de engajamento e nas escolhas sobre quais dados coletar e como utilizá-los.

Empresas que desenvolvem soluções digitais possuem hoje uma capacidade sem precedentes de influenciar

comportamentos. Com esse poder vem uma responsabilidade proporcional. Se uma plataforma sabe que parte relevante de sua audiência é composta por crianças e adolescentes, ela não pode tratar a proteção desse público como um item secundário ou apenas como uma exigência regulatória.

Outro aspecto importante é a própria participação da sociedade no processo de fiscalização. Ao criar um canal específico para denúncias, a ANPD reconhece que os reguladores não conseguem identificar sozinhos todas as situações de risco existentes no ambiente digital. A colaboração dos cidadãos passa a funcionar como um mecanismo complementar de monitoramento e aperfeiçoamento das políticas públicas.

Isso não significa transformar cada usuário em fiscal. Significa reconhecer que a proteção de direitos fundamentais depende da atuação conjunta de diversos agentes. Quanto mais informações qualificadas chegam aos órgãos responsáveis, maior a capacidade de identificar padrões de comportamento e direcionar ações regulatórias de forma eficiente.

Para as empresas, a mensagem é clara. A conformidade com o ECA Digital não deve ser vista apenas como uma obrigação legal. Ela representa uma oportunidade de demonstrar compromisso genuíno com a proteção de usuários vulneráveis. Organizações que incorporam segurança, privacidade e transparência desde a concepção de seus produtos fortalecem sua reputação e constroem relações mais sólidas com a sociedade.

A tecnologia continuará avançando. Novas plataformas surgirão, novos modelos de negócio serão criados e novos desafios aparecerão. O que não pode mudar é o princípio de que a inovação deve caminhar lado a lado com a proteção das pessoas. E quando falamos de crianças e adolescentes, essa responsabilidade se torna ainda maior. Afinal, o futuro digital que estamos construindo hoje será o ambiente em que as próximas gerações irão crescer.

Saiba quem é a nossa Colunista:

Denise Debiasi é CEO da Bi2 Partners, reconhecida pela expertise e reputação de seus profissionais nas áreas de investigações globais e inteligência estratégica, governança e finanças corporativas, conformidade com leis nacionais e internacionais de combate à corrupção, antissuborno e antilavagem de dinheiro, arbitragem e suporte a litígios, entre outros serviços de primeira importância em mercados emergentes.

Como governar agentes de IA e controlar seus custos nas empresas

Toda grande equipe de corrida já foi, em algum momento, apenas uma garagem cheia de máquinas potentes e pilotos talentosos

George Tani (*)

A potência estava ali. Faltava coordenação. Sem alguém no comando do pit e sem um plano de corrida comum, cada carro seguia o próprio traçado, transformando potencial em batida. A Inteligência Artificial (IA) começa a colocar as empresas exatamente diante desse desafio. Depois da corrida para criar agentes capazes de executar tarefas de forma autônoma, surge uma pergunta muito mais estratégica: quem está com as mãos no volante?

Um exemplo recente ajuda a explicar essa mudança. Em 2026, a Uber ampliou o acesso de seus engenheiros a ferramentas baseadas em agentes de IA para desenvolvimento de software. A adoção cresceu rapidamente, porém o consumo de tokens avançou em ritmo ainda maior, levando a companhia a consumir, em poucos meses, todo o orçamento anual destinado àquelas ferramentas. O episódio chamou atenção porque não representava um fracasso da tecnologia, mas exatamente o contrário. Os agentes funcionavam tão bem que passaram a ser utilizados em escala muito superior ao previsto. O problema deixou de ser tecnológico e passou a ser de gestão.

Esse cenário tende a se tornar comum. Uma pesquisa estima que, até 2028, cerca de 33% dos softwares corporativos incorporarão agentes de IA, contra menos de 1% em 2024. A projeção indica ainda que, aproximadamente, 15% das decisões rotineiras de trabalho serão tomadas por esses sistemas no mesmo período. Ao mesmo tempo, alerta que mais de 40% dos projetos de IA Agêntica poderão ser cancelados até 2027 por falta de valor claro, controles inadequados ou custos elevados. O desafio deixou de ser construir agentes inteligentes. O desafio passou a ser coordená-los.



peskow_caiwa

É justamente aqui que a analogia das pistas revela toda a sua força. Uma organização não fracassa porque tem muitas máquinas potentes na garagem: ela fracassa quando cada uma corre uma prova diferente. O mesmo acontece com agentes de IA desenvolvidos de forma isolada por diferentes áreas do negócio. Recursos Humanos cria um assistente para políticas internas. Finanças desenvolve outro para análises. Jurídico implementa um terceiro para apoiar questões regulatórias. Tecnologia cria dezenas de agentes especializados. Individualmente, todos podem ser excelentes, cada um entregando como o motor seis-cilindros aspirado de um Porsche 911 ou o câmbio manual preciso de um BMW classe M. Coletivamente, contudo, podem gerar redundância, respostas inconsistentes, desperdício de recursos e uma crescente dificuldade para saber quem faz o quê.

A maioria das organizações ainda está aprendendo essa lição. Um estudo mostra que apenas 8% das empresas possuem uma estrutura abrangente de governança para IA. Outra pesquisa revela que somente 21% mantêm um inventário atualizado dos agentes ativos em seus ambientes. É como assumir o comando do pit sem saber quantos carros estão na pista ou qual estratégia cada piloto está seguindo.

E é aqui que vale um ajuste importante na própria analogia. O estrategista

não inventa a corrida no meio da prova. Antes da luz verde existe um plano de corrida, uma ficha de acerto conhecida por toda a equipe. Nas companhias, esse acerto é a governança. Ela define quais agentes podem ser criados, quais dados podem utilizar, quais decisões podem tomar, quem responde por seus resultados e quais limites financeiros e operacionais precisam ser respeitados. O líder responsável pela IA exerce o papel de chefe de equipe justamente porque garante que todos os agentes sigam o mesmo plano de corrida.

Os custos fazem parte dessa equação, mas não são sua essência. O preço médio dos tokens vem caindo rapidamente, enquanto o consumo cresce em velocidade ainda maior. Segundo um levantamento, 73% das organizações afirmam que os gastos com IA superaram as expectativas. A disciplina conhecida como FinOps, originalmente criada para a computação em nuvem, começa agora a ser adaptada para a IA justamente porque controlar apenas o preço deixou de ser suficiente. O que importa é compreender quanto valor cada agente entrega em relação aos recursos que consome.

Essa mudança também redefine o papel da liderança. Durante décadas, executivos aprenderam a administrar organizações compostas apenas por pes-

soas. Agora, eles passam a conduzir ambientes onde pessoas e agentes inteligentes trabalham lado a lado. O gestor deixa de supervisionar somente atividades humanas para coordenar um ecossistema híbrido, no qual parte das decisões, análises e execuções ocorre de forma autônoma. A competência mais importante deixa de ser acompanhar cada tarefa individualmente e passa a ser desenhar boas regras, estabelecer prioridades e criar mecanismos que mantenham todo o sistema funcionando em sincronia, como uma equipe bem entrosada no box.

A boa notícia é que governança não reduz inovação: ela a torna escalável. Assim como um bom chefe de equipe não tira o talento do piloto, mas cria as condições para que a máquina entregue tudo o que tem, uma boa estrutura de governança permite que agentes de IA evoluam com segurança, transparência e eficiência. Definir responsáveis, acompanhar indicadores, estabelecer orçamentos, monitorar riscos e aposentar agentes que deixaram de gerar valor não representa burocracia. E isto representa maturidade.

Nos próximos anos, praticamente toda grande empresa terá uma verdadeira frota de agentes de IA executando atividades críticas do negócio. A diferença entre as companhias que capturarão valor e aquelas que apenas acumularão custos dificilmente estará na quantidade de agentes em operação, mas sim na qualidade de quem está no comando do pit. Porque agentes inteligentes tendem a se tornar uma commodity, assim como cavalos de potência hoje se compram aos milhares. O que continuará raro será a capacidade de fazer todos eles correrem a mesma prova, seguindo o mesmo traçado.

(*) Diretor CRM e PaaS da GFT Technologies no Brasil.

Segurança condominial entra na era da inteligência

Andre Mario (*)

O mercado condominial tem passado por uma grande transformação no país. Especialmente nas grandes cidades, a portaria remota ou portaria virtual vem substituindo o capital humano. A economia de custos e passivos trabalhistas motivaram essa mudança em curso. Moradores logo se adaptam, contudo, essa transformação digital traz o desafio de unir a eficiência à segurança, não apenas contra roubos, mas pensada também contra incêndios. A figura do zelador atento deixa de existir e é aí que a vigilância ganha mais uma mão da tecnologia, por meio dos alarmes de incêndio sem fio. Essa integração protege vidas e reduz custos operacionais sem a necessidade de grandes reformas estruturais.

Cada vez mais, assim, a tecnologia assume o papel de guardiã total da edificação, especialmente em situa-

ções de sinistro. Tradicionalmente, os sistemas de detecção de fogo dependiam de quilômetros de cabos embutidos nas construções. Hoje, os dispositivos com comunicação via radiofrequência ou rede sem fio revolucionam essa lógica, não só pelo fato de não mais precisar alterar a arquitetura original do edifício, como também pelo fato dos dados de cada sensor responderem de maneira muito mais rápida e inteligente, permitindo um alcance robusto no atendimento à segurança.

O ponto central da inovação é a comunicação direta entre o alarme de incêndio e o software de controle de acesso da portaria remota. Assim, quando um detector capta fumaça ou o botão de pânico é acionado, o sistema inteligente destrava automaticamente todos os portões de saída e rotas de fuga.

Simultaneamente, o alerta chega em segundos à central de monito-

ramento externa, que aciona imediatamente o Corpo de Bombeiros, garantindo uma resposta rápida no local.

Edifícios residenciais ou comerciais que escolham a portaria remota como controle de acesso podem e devem buscar redução de despesas nessa transformação.

Contudo, jamais negligenciar com a segurança da edificação. Se a tecnologia pode substituir a ação humana em certas atividades, a inovação em conceitos de segurança deve, igualmente, fazer parte desse planejamento. Os alarmes de incêndio estão contemplados nesse conceito de inovação e merecem dos gestores a devida atenção. De perto ou de longe, a segurança de todos que ali habitam, circulam ou trabalham sempre deve ser priorizada.

(*) CEO da Wi Fire sistema de alarme wireless com 14 anos de mercado. Economista formado pela USP, com MBA em Finanças.