POR:
Rui Almeida e Vânia Soares

MONERIS

OS DESAFIOS DA PRIVACIDADE NO NOVO NORMAL

O SURTO PANDÉMICO DE SARS-COV-2, ASSIM COMO AS MEDIDAS DE CONFINAMENTO QUE O ACOMPANHAM, MUDARAM DRAMATICAMENTE A VIDA DE TODOS NÓS

As perspectivas económicas mundiais e o curso da vida empresarial alteraram-se de forma dramática e imprevisível, obrigando pessoas e empresas a adaptarem-se em poucos dias, semanas ou meses. Quem não se conseguiu ou conseguir rapidamente adaptar, dependendo do sector ou mercado em que actua, já está ou estará inevitavelmente condenado a definhar.

A evidente resposta a todo este novo enquadramento, que nos obriga a distanciamento social e à adopção forçada do modo remoto é, claramente, a tecnologia. E com a crescente dependência da tecnologia, que se acentuou de forma transversal com a crise pandémica, a tensão entre o aumento da utilização de dados (muitos dos quais pessoais, e outros tantos sensíveis) e as restrições ao seu tratamento e divulgação impostas pelos princípios de privacidade e da protecção de dados, colocam-nos a todos desafios de primeira ordem.

OS DEPARTAMENTOS DE IT ENFRENTAM DESAFIOS NOVOS E ACRESCIDOS, UMA VEZ QUE A FORÇA DE TRABALHO DE MUITAS EMPRESAS FOI ENVIADA PARA CASA PARA TRABALHAR REMOTAMENTE

A mediação de interesses e direitos contraditórios, como sejam o direito à privacidade ou à liberdade de movimentação, e a protecção do direito à saúde ou ao estado social, será feita em cada país de forma diferente. Trata-se de compromissos difíceis de assumir, mas que conjunturalmente poderão ter uma avaliação distinta daquela que estruturalmente se considerará a mais adequada.

Também nos vários sectores e actividades económicas, os reguladores adoptaram abordagens distintas para enfrentar esta crise. Em especial, as entidades reguladoras no âmbito da privacidade e protecção de dados, têm procurado transigir num conjunto de princípios que antes tinham sido dados como essenciais, de modo a acomodar a necessidade de responder à crise sanitária, e por forma a não serem vistos como obstáculos à tomada de medidas que permitam salvaguardar a saúde pública. O papel percebido e desempenhado

ABORDAGENS
NOS VÁRIOS SECTORES E ACTIVIDADES ECONÓMICAS, OS REGULADORES ADOPTARAM ABORDAGENS DISTINTAS PARA ENFRENTAR ESTA CRISE

moneris

pelos reguladores europeus independentes mais consolidados foi o de agir no interesse público, e o de adaptar a sua abordagem de modo a assegurar que esta se mantém pragmática e proporcional. Mas é importante perceber que vivemos tempos excepcionais e que esta indulgência tem os dias contados e não é ilimitada.

Por outro lado, para muitas entidades que dependem hoje da tecnologia para a continuidade da prossecução dos seus objectivos e do seu propósito, torna-se ainda mais imperativo garantir a observância de processos e sistemas desenhados para proteger a privacidade e os dados pessoais dos seus colaboradores, clientes ou demais stakeholders. É este o caso da, a título de exemplo, área da educação, a área da saúde ou o sector financeiro, para mencionar apenas alguns. A reputação e a confiança são essenciais para quem desenvolve a sua actividade de forma principal ou com especial incidência no ambiente digital e para quem trata dados pessoais e tem especial recorrência nas actividades de tratamento de dados sensíveis.

Os departamentos de IT enfrentam assim desafios totalmente novos e acrescidos, uma vez que grande parte ou toda a força de trabalho de muitas empresas foi enviada para casa para trabalhar remotamente. Estes departamentos devem assim assegurar a segurança dos seus sistemas, softwares e dados fora da rede corporativa, ao mesmo tempo que satisfazem os requisitos do

» Rui Almeida, CEO da Moneris

» Vânia Soares, business developer da Moneris

Regulamento Geral de Protecção de Dados (RGPD) em matéria de protecção contra eventuais ataques cibernéticos. Os colaboradores das empresas estão hoje, em muitos casos, a utilizar ligações individuais para se conectarem às redes corporativas, enquanto os departamentos de IT tentam salvaguardar a expansão rápida e não planeada das infra-estruturas de apoio. Os controlos e processos estão assim fragilizados e os riscos e ameaças cibernéticas estão à espreita.

O Centro Nacional de Cibersegurança alertou já para o aumento exponencial de ciberataques. Desde o início da pandemia, muitas foram as campanhas de informação e sensibilização veiculadas para empresas e particulares, de que é exemplo a campanha de phishing (por email, SMS ou redes sociais), a divulgação de plataformas digitais ou de aplicações para dispositivos móveis que de forma oculta estão orientadas para a infecção dos seus equipamentos com malware, inclusive da tipologia ransomware, esquemas de fraude digital divulgados por mensagem electrónica ou nas redes sociais, SMS não legítimos, entre outros.

COM A CRESCENTE DEPENDÊNCIA DA TECNOLOGIA, QUE SE ACENTUOU COM A CRISE PANDÉMICA, A TENSÃO ENTRE O AUMENTO DA UTILIZAÇÃO DE DADOS E AS RESTRIÇÕES AO SEU TRATAMENTO E DIVULGAÇÃO, COLOCAM-NOS A TODOS DESAFIOS DE PRIMEIRA ORDEM

Neste contexto, o RGPD, em vigor há mais de dois anos, mas com a lei de execução portuguesa aprovada há pouco mais de um, ganhou uma relevância acrescida e um impacto real no dia-a-dia das pessoas e das organizações.

Mais do que cumprir uma obrigação legal e recear as (pesadas) multas previstas por incumprimento, os empresários e gestores devem considerar os benefícios e o valor intrínseco do investimento na segurança e privacidade dos

dados, assim como devem ser capazes de percepcionar como este investimento pode beneficiar a sua organização. Construir uma segurança da informação madura e um programa de protecção de dados robusto pode enaltecer o profissionalismo dos colaboradores de uma empresa e reforçar a sua reputação pública.

Nesta cruzada para garantir a privacidade e a protecção de dados, há dois campos de batalha igualmente importantes, igualmente expostos, igualmente indispensáveis – a tecnologia e as pessoas.

No campo da tecnologia, efectivamente, a privacidade de dados tem uma importância acrescida na protecção contra o crime cibernético. Estar em conformidade com o RGPD significa ter bem definidas as finalidades para a recolha de dados pessoais (higienizar os dados pessoais), proteger a informação sensível e apostar em softwares que removam informação fora de validade.

O Artigo 32.º do RGPD, que fala sobre os requisitos de segurança, exige que as empresas e organizações, públicas e privadas, sejam cada vez mais estruturadas e formais na forma como é organizada a informação pessoal, incluindo finalidades bem definidas para a recolha, transparência, minimização de dados e apoio aos direitos dos titulares de dados.

É aqui que entramos no campo das pessoas. Considerando que a maioria das violações de dados resulta de erro humano, é facto que a formação, informação e sensibilização dos recursos humanos é a pedra de toque de todo o procedimento de conformidade ao RGPD.

AS ORGANIZAÇÕES QUE SE ENCHEM COM FERRAMENTAS E COMPETÊNCIAS MAIS ROBUSTAS E INTEGRADAS DE CIBERSEGURANÇA IRÃO, NO MÉDIO-LONGO PRAZO, TER AQUI UM FACTOR COMPETITIVO E DE DIFERENCIAÇÃO QUE AS POSICIONARÁ ACIMA DOS SEUS CONCORRENTES

Por isso se torna fundamental a estruturação de processos nas empresas que garantam a máxima eficácia na aplicação das políticas internas de protecção de dados. Para que os colaboradores de uma empresa possam gerir a informação pessoal numa base diária, é necessário garantir um completo programa de awareness e formação, sendo que a combinação entre privacidade de dados e cibersegurança se tem tornado uma best practice.

A cibersegurança deixou de ser um tema exclusivo das TI e passou a estar no topo das preocupações da direcção executiva das organizações. Além dos aumentos consideráveis no investimento direccionado ao combate ao cibercrime, há também uma tendência para um aumento no tempo e recursos dedicados a este tema.

O respeito pela privacidade e protecção de dados, com práticas bem estruturadas e uma equipa alinhada nesta visão, pode trazer benefícios directos em novas oportunidades de receita, ou na redução de custos de armazenamento e de oportunidade (ter sempre a informação localizada e actualizada), mas tem sobretudo reflexo no valor intrínseco da organização, na sua reputação, na sua credibilidade.

Trabalhar de forma sistemática e profissional na protecção de dados significa perceber os riscos, assim como direccionar esforços e investimento para as áreas certas. As organizações que o fazem retiram dividendos noutras áreas da empresa, como sejam a Gestão de Risco e Responsabilidade Corporativa, as Operações de Controlo de Dados e as Relações com clientes, colaboradores e stakeholders.

Seguramente, as organizações que se apetrecharem com ferramentas e competências mais robustas e integradas de cibersegurança irão, no médio-longo prazo, ter aqui um factor competitivo e de diferenciação que as posicionará acima dos seus concorrentes. E, mais importante, um forte compromisso com a cibersegurança permitirá às empresas emergir mais fortes e melhor preparadas para lidar com futuras perturbações de grande escala e com a realidade do novo normal, que veio para ficar. ●