Recibido: septiembre 2020/Aceptado: enero 2021

Anuario Facultad de Ciencias Económicas y Empresariales
ISSN 2218-3639

Proteção de dados como diferencial competitivo nas empresas angolanas

Data protection as a competitive differential for Angolan companies

Ph.d. Mendes Pedro-Ludi, ludi305@gmail.com, https://orcid.org/0000-0002-6972-0394;
Dr. C. Maricela Arias-Madrazo, marias@uo.edu.cu, https://orcid.org/0000-0003-3688-9051

Universidade Agostinho Neto, Luanda, Angola;
Universidad de Oriente, Santiago de Cuba, Cuba

Resumo

O surgimento das Tecnologias de Informação e Comunicação traz em si uma ameaça iminente à penetração de bancos de dados confidenciais de instituições públicas e privadas, por conhecidos "hackers" que nos últimos anos têm causado escândalos em todo o mundo. Em Angola, de momento, não existe uma cultura de protecção de dados pessoais e oficiais nas instituições, públicas ou privadas, pois não se sabe que a protecção de dados contribui significativamente para a redução de custos e, por isso, deve ser valorizada como uma vantagem competitiva para as instituições, de acordo com a lei de proteção de dados pessoais. O objectivo deste artigo é fornecer uma base teórica sobre aspectos relacionados com a protecção de dados pessoais e promover uma cultura de protecção de dados nas instituições públicas e privadas angolanas, considerando a protecção de dados como um diferencial competitivo e não como uma despesa adicional para instituições.

Palavras-chave: Protecção de dados, vazamento de dados, factor de competitividade, factor de oportunidade, custo de oportunidade e avaliação de risco.

Abstract

The emergence of Information and Communication Technologies carries in itself an imminent threat to the penetration of confidential databases of public and private institutions, by well-known "hackers" who in recent years have caused scandals throughout the world. In Angola, at the moment, there is no culture for the protection of personal and official data in institutions, - public or private - as it is not known that data protection contributes significantly to reducing costs and therefore, should be valued as a competitive advantage for institutions, in compliance with the personal data protection law. The objective of this article is to provide a theoretical basis on aspects related to the protection of personal data and to promote the creation of a culture of data protection in Angolan public and private institutions, considering data protection as a competitive differential and not as an additional expense for institutions.

Keywords: Data protection, data leakage, competitiveness factor, opportunity factor, opportunity cost and risk assessment.

Introdução

Com a utilização massiva das novas tecnologias de informação e comunicação a nível mundial e em particular em Angola, as empresas, por menores que sejam, têm que proteger os seus dados como forma de salvaguardar, garantir a sua integridade e segurança.

Neste sentido, as vantagens da utilização das novas tecnologias de informação e comunicação (TIC) implicam implicitamente na ameaça iminente de penetração de bases de dados confidenciais de instituições públicas e privadas, por intrusos, mais conhecidos como "hackers", que em últimos anos causaram vários escândalos em todo o mundo, entre os quais podemos citar: Panama Papers (2015), hotéis Marriott (2014 e 2018), Google+ (2018), Amazon (2019) e o caso Luanda Leaks (2019) entre outros.

Embora este mal afecte muitos países do mundo, e se apliquem os correspondentes mecanismos de protecção e segurança, em Angola ainda não existe uma cultura de protecção de dados pessoais nas instituições, sejam públicas ou privadas.

O objectivo deste artigo é fornecer uma base teórica sobre aspectos relacionados com a protecção de dados pessoais e promover uma cultura de protecção de dados nas instituições públicas e privadas angolanas, considerando a protecção de dados como um diferencial competitivo e não como um gasto adicional para as instituições.

A metodologia de investigação utilizada assenta em métodos científicos e categorias de conhecimento, nomeadamente o método histórico-lógico, análise-síntese, resumo-concreto, indução-dedução, bem como a revisão bibliográfica, principalmente por via eletrónica.

Fundamentação teórica

A década de 1990 marcou o início da adesão massiva das novas tecnologias de informação, e hoje não há dúvida que a sociedade atual optou pelo uso massivo da engenharia elétrica para a realização de operações como: transações financeiras, trabalho remoto (utilização de espaços de coworking e home office), que se tornaram uma tendência mundial e até na gestão pública, cujo uso tem ocasionado nos últimos anos, um aumento alarmante de ataques virtuais, incluindo roubo, alterações e vazamento de dados.

Nesse sentido pode-se afirmar (Positivo, 2019), que as evidências reforçam como indiscutível, e é que com quase todos os ativos financeiros e informacionais dos cidadãos.

na nuvem - e muito poucos fisicamente - os criminosos de violação de dados digitais se intensificam; O crime cibernético está se tornando mais sofisticado e uma ameaça permanente para a economia do planeta, causando um custo estimado de segurança digital de acordo com o Fórum Económico Mundial de 8 triliões de dólares (estimado até 2024).

Os ataques e crimes informáticos infectaram 300 mil computadores simultaneamente numa ação coordenada de hackers para a União Europeia em 2017 (Wanna Cry), suspendendo o serviço em hospitais, bancos e até tribunais. Desde então, já foram registrados milhares de casos individuais no mundo, segundo denúncias feitas no site do Infobae.

Por este motivo, o investimento em equipamentos de protecção e políticas de segurança da informação tornou-se uma prioridade e não uma opção como se pensava anteriormente. Consequentemente, Angola não pode e não deve ser excluída da realidade de acontecimentos desta natureza.

Uma prova do perigo que correm as instituições públicas e privadas angolanas nesta matéria é o recente caso de fuga de dados, relativo às empresas da empresária angolana Isabel dos Santos, - conhecido como o caso Luanda Leaks, - publicado pela primeira vez em 19 de janeiro de 2020. A informação foi divulgada através de uma ação do hacker português "Rui Pinto".

Isto, por si só, revela que o vazamento de informações em instituições públicas e privadas, e de indivíduos, é internacional; ou seja, os criminosos não precisam residir no país onde a acção criminal é cometida, o que torna ainda mais complexo e perigoso detectar e prevenir.

A protecção dos dados pessoais confere confidencialidade e reservas da vida privada e é de fundamental importância no contexto da salvaguarda dos direitos fundamentais dos cidadãos, reconhecidos pela Declaração Universal dos Direitos do Homem e pela Carta Africana dos Direitos do Homem e os povos, neste caso particular, dos países africanos.

A consagração na Constituição da República de Angola, ao direito à preservação da privacidade e à possibilidade de recurso à disponibilização de "habeas data", representa claramente um passo importante na adopção de um quadro legislativo nesta matéria.

O direito à privacidade também se traduz no respeito pela privacidade dos cidadãos no que diz respeito ao tratamento dos dados pessoais que lhes dizem respeito. Embora este tratamento tenha um papel relevante na melhoria do bem-estar dos cidadãos e do

progresso económico, num contexto de promoção e desenvolvimento de uma maior variedade de serviços, nomeadamente no domínio das tecnologias e da sociedade da informação, é preciso garantir o que é feito respeitando a privacidade.

A Lei de Protecção de Dados Pessoais (Lei n.º 22/11, de 17 de junho), o Estatuto Orgânico da Agência de Proteção de Dados (Decreto Presidencial n.º 214/16, de 10 de outubro) e a Lei de Protecção de redes e sistemas informáticos (Lei n.º 7/17, de 16 de fevereiro) são instrumentos criados pelo Estado angolano para garantir a aplicação da protecção de dados pessoais, nos termos do artigo 3.º (Âmbito de aplicação subjectivo e territorial) da Lei de Protecção que estabelece o seguinte:

1. O tratamento de dados pessoais por qualquer pessoa e entidade do sector público, privado ou cooperativo está sujeito a esta lei.

2. Esta lei se aplica ao processamento de dados pessoais realizado:

a) Pelo responsável pelo tratamento sedeado na República de Angola;

b) No âmbito da actividade do controlador responsável pelo tratamento estabelecido na República de Angola, ainda que o referido controlador não tenha a sua sede em território angolano;

Fora da República de Angola, onde a lei angolana seja aplicável ao abrigo do direito internacional público ou privado;

d) Pelo responsável pelo tratamento que, não estando estabelecido na República de Angola, utilize, para o tratamento de dados pessoais, os meios localizados em território angolano.

3. Para efeitos da alínea a) do n.º 2, considera-se que o responsável pelo tratamento utiliza recursos localizados em território angolano quando é efectuado o tratamento de dados pessoais ou quando os dados pessoais se encontram alojados, em meio situado em território angolano; Para os efeitos da presente lei, basta a simples utilização dos referidos meios para a recolha, registo ou trânsito de dados pessoais no território da República de Angola.

4. No caso da alínea d) do n.º 2, o responsável pelo tratamento deve designar, mediante comunicação à Agência de Protecção de Dados, um representante estabelecido na República de Angola para o substituir em todos os seus direitos e obrigações, sem prejuízo dasua responsabilidade própria.

O anterior mostra que, em geral, a credibilidade das instituições públicas e a permanência das instituições privadas no mercado mundial e, em Angola em particular, dependerá da visão que se adapte a partir de agora, da necessidade de protecção dos recursos. Dados pessoais, considerando-os um factor de competitividade e não um mero gasto, visto que, actualmente, o procedimento visa garantir a confiança dos clientes no que diz respeito à protecção dos dados pessoais detidos pelas instituições.

No entanto, a evolução muito marcante na área das TIC, demonstrada em pesquisas realizadas por especialistas e autores no assunto, suas vulnerabilidades e a necessidade de protecção de dados pessoais versus cibersegurança, permitiu a este pesquisador concluir que a utilização das novas tecnologias e o sucesso das TICs baseia-se no reconhecimento da protecção de dados como um diferencial competitivo, para o qual é necessário avaliar quatro (4) factores essenciais:

1. Oportunidade.

2. Avaliação do risco de vazamento de dados.

3. Custo de oportunidade.

4. Competitividade.

Métodos usados

A pesquisa foi possível graças à aplicação de métodos científicos e categorias de conhecimento, em particular os métodos histórico-lógico, análise-síntese, concreto-abstrato, indução-dedução.

Abstração científica, para analisar as particularidades do fenómeno estudado, despojado da influência de outros fenómeno e sua concretização refletida na síntese destes. A análise e síntese para detalhar e integrar os modelos, definições e conceitos relacionados com a Protecção de Dados Pessoais, bem como a Lei da Protecção de Dados Pessoais em vigor em Angola, combinada com o método histórico lógico na análise dos antecedentes das novas tecnologias da informação e seu impacto nas instituições públicas e privadas desde seu surgimento, evolução, desenvolvimento e introdução em vários países do mundo.

Aplicam-se a indução e a dedução, como forma de raciocínio na pesquisa, por meio da qual o conhecimento do objecto de estudo e de cada um dos elementos abordados com suporte na bibliografia consultada, permite confirmar a inter-relação destes e as bases teóricas para a sua implementação em instituições públicas e privadas em Angola.

Resultados e discussão

O argumento resultante ao avaliar os 4 factores de sucesso como diferenciais competitivos para a protecção de dados pessoais na utilização das TIC, é explicitado em cada um deles, com base nos principais documentos analisadosnesta pesquisa.

Factor de oportunidade

A regulamentação na União Europeia (UE) em abril de 2016 do Regulamento Geral de Protecção de Dados (GDPR), abriu caminho para que outros países do mundo adotassem ou adaptassem sua própria Lei de Protecção de Dados, como é o caso do Brasil. , Cabo Verde, São Tomé e Príncipe, só para citar alguns países onde a aplicação desta lei já é uma realidade, resoluções que trouxeram e impactarão o funcionamento de aplicativos móveis, sites e plataformas, que actuam diretamente na colecta, análise e utilização de dados pessoais. Por isso, empresas que não conseguirem proteger os dados de seus clientes, seja por falta de conhecimento ou de capacidade técnica e financeira, perderão competitividade ao perderem oportunidades.

Consequentemente, é necessário que as instituições sejam atempadas e dinâmicas face ao surgimento de novas tecnologias e novas técnicas de ataque de hackers, para garantir a segurança dos dados pessoais dos seus clientes e para acompanhar as exigências do mercado.

É necessário imediatamente - e vale ressaltar -, considerar as 5 acções que podem ser apreendidas a partir dos casos de violação de dados ocorridos (em 2018, 2019) citados pelo Positivo (2019, site www.meupositivo.com.br) intitulados "5 lições que podemos aprender com os escândalos de vazamento de dados".

1. Não espere um ataque de hacker para implementar políticas de segurança da informação. Antecipe, a prevenção deve ser a medida mais eficaz para controlar e ccmonitorar a segurança e protecção das informações.

O site argumentou que em uma pesquisa aplicada foi revelado que 56% das empresas solicitam ajuda para protecção de dados somente após o primeiro ataque. Por isso, recomenda desenvolver controlos de acesso em sistemas, investindo em soluções em nuvem com recursos de backup automático e implementando protecções como firewall, IDS, IPS, além de Internet devido à alta velocidade e capacidade de tráfego.

2. Capacite os funcionários. Isso nada mais é do que manter a preparação, e indicações permanentes aos funcionários, para o uso adequado dos sistemas instalados; Mesmo

quando apresentam um aviso de segurança ou perigo ao desproteger os dados, o uso de senhas fáceis e vulneráveis, a abertura de arquivos maliciosos, bem como a prática incorreta de deixar a sessão aberta fora do seu horário de trabalho.

Todas estas e outras vulnerabilidades não são apenas comuns a Angola, mas a muitos utilizadores no mundo, o que se evidencia nos resultados dos inquéritos realizados pela Trustwave (2017) que não só mostraram, mas também demonstraram que um grande número de casos de vazamentos de dados são consequências das vulnerabilidades geradas pelo uso indevido dos sistemas, entre as quais as expressas anteriormente.

3. Aumente a segurança dos dados conforme a tecnologia avança. Nesse sentido, refere-se às vantagens do 5G em termos de acesso e transmissão de dados muito mais rápidos, e às possibilidades de fábricas inteligentes, cirurgias remotas, entre outras, em termos de maior capacidade de conexão, maior probabilidade de crescimento de ataques DDoS .

Neste sentido, as instituições em geral, e em particular as empresas que investem no aumento da largura de banda, são aconselhadas a utilizar uma firewall gerida para monitorização em tempo real e a estudar a implementação do denominado "debugging center", station limpeza centralizada de dados, onde o tráfego de rede e os aplicativos são analisados para eliminar acções maliciosas.

4. Nunca ignore os sinais de advertência. Eles simplesmente não podem ser ignorados, pois se as empresas possuem sistemas de controlosinternos que permitem identificar suas vulnerabilidades, estes devem assumi-las como riscos, fornecer acompanhamento e monitoramento constantes e aplicar de forma adequada.

medidas de prevenção imediatas e acções eficazes para eliminar ou corrigir o impacto de actividades maliciosas que afectam seu sistema de tecnologia da informação.

5. Actualize seu parque tecnológico. Esta quinta recomendação refere-se aos benefícios dos modernos sistemas de segurança digital, que incluem inteligência artificial para monitoramento da rede; Portanto, recomenda como garantia o acesso a essas tecnologias, investindo em infraestrutura de TI, eliminando as obsoletas.

Só a relação custo-benefício já explica esta quinta recomendação, pois é óbvio que o custo de aquisição de computadores e tecnologias modernas (celulares, smartphones, tablets ou acessórios) é menor que o custo de seu conserto e recuperação, em caso de um ataque cibernético.

A segurança, oportunidade da protecção dos dados pessoais, embora não seja infalível, está a indicar que devem ser criados mecanismos para antecipar a vulnerabilidade por um ataque pirata ou outras formas de violação da segurança dos dados privados e públicos, lição que deixou em 2018, a colecta ilegal de dados pela Cambridge Analytica, (Positivo, 2019) afectou mais de 87 milhões de usuários do Facebook, o que significou uma multa de 643 mil dólares por violação de privacidade.

Avaliação de risco de vazamento de dados

A avaliação dos riscos inerentes à utilização das TIC é um pressuposto incontornável no mundo da cibernética, após a avaliação do risco operacional, visto ser uma componente de controlo, estabelecendo as bases para a identificação, avaliação e análise dos riscos que as agências, organizações e entidades enfrentam no cumprimento de seus objectivos.

Uma vez classificados os riscos em internos e externos, por processos operacionais, financeiros, tecnológicos e outros inerentes ao tipo de actividade, são avaliadas as principais vulnerabilidades, determinados os objectivos de controlo e estabelecido o plano de prevenção e mitigação deriscos, definindo a forma como serão geridos.

O impacto de ataques cibernéticos e crimes tornou-se muito importante não só no sector financeiro onde eles começaram em 1990, mas em outros segmentos do mercado de Tecnologia da Informação (TI), como projectos, construção, desenvolvimento, para citar alguns. Portanto, a mitigação de riscos operacionais de importância, passou a ser uma necessidade e prioridade no plano de controlo e prevenção de riscos nas entidades.

As lições aprendidas com a insolvência de várias instituições bancárias nos anos 90, que afectou a sua imagem e reputação e, consequentemente, minou a confiança no mercado em negócios de grande importância, tornaram-se parâmetros de vigilância e monitorização para as empresas. .

Em resposta a essas lições, as instituições bancárias passaram a identificar os riscos inerentes ao seu negócio, traçando possíveis soluções para eliminar ou mitigar o risco e bloquear qualquer tipo de impacto negativo que eles poderiam trazer, definindo essas acções como "boas práticas" em várias organizações.

Nesse sentido, é importante diferenciar mitigação e risco. Mitigar significa desacelerar, amortecer, atenuar. Por outro lado, a palavra risco está associada à incerteza de que ocorrerá um evento que possa afectar (ou beneficiar) o alcance dos objectivos; algo que provavelmente ocorrerá. A partir daí, a empresa deve estar preparada para identificar e

eliminar tudo que possa impactar negativamente a rotina operacional a médio e longo prazo, sejam problemas de segurança, mau funcionamento do sistema ou falhas em procedimentos internos, e consequentemente elaborar e monitorar uma política de mitigação de riscos, que se enquadram nos chamados riscos operacionais.

Quando se fala em mitigação de riscos operacionais, faz-se referência ao "risco de perda por inadequação ou falha de processos internos, pessoas e sistemas ou por causas de eventos externos" (BCBS, 2004: 128), portanto, refere-se à mitigação dos impactos que uma falha processual pode trazer para a instituição.

A falta de segurança da informação cria brechas para o vazamento de dados estratégicos do negócio, por exemplo, quando ocorre a falha, a empresa está sujeita a perder capital e ter prejuízo financeiro.

Existem vários tipos de riscos operacionais que podem ocorrer ao longo da vida de uma empresa, desde uma simples falha de produção até uma grande fraude. O tipo de impacto causado está relacionado à gravidade do risco e ao nível de preparação da organização para combatê-lo. De acordo com a pesquisa realizada, as principais consequências de um risco mal dimensionado são:

a) perda de credibilidade da instituição, como ocorreu com os bancos na década de 1990;

b) perda financeira, que pode comprometer o futuro e a sustentabilidade da organização.

A tecnologia da informação (TI) também tem seus próprios riscos operacionais, que estão especificamente relacionados aos principais atributos de seus activos. A bibliografia consultada reconhece pelo menos três atributos fundamentais para mitigar os riscos de TI, que são: confidencialidade, integridade e disponibilidade.

1. Confidencialidade: consiste em garantir o controlo de acesso às informações, garantindo que haja um critério de disponibilidade, uma vez que os riscos a que está sujeita a confidencialidade estão relacionados à invasão, ou seja, ao acesso não autorizado por terceiros - membros ou não da instituição -.

A falta de controlo da confidencialidade sujeita à instituição, acarreta perda de clientes e oportunidades de negócios, riscos de fraude e danos à imagem da empresa, tanto interna quanto externamente.

2. Integridade - garante que os dados estejam estáveise protegidos contra perdas e danos devido a falhas de hardware e software. Além disso, se a confidencialidade for violada,

com indivíduos autorizados e não autorizados suspendendo indevidamente as informações, as informações podem ser alteradas propositalmente ou inadvertidamente.

Como os problemas relatados acima, danos à integridade podem causar danos incalculáveis a uma empresa. Imagine perder ou danificar informações estratégicas, como histórico financeiro e dados críticos de contabilidade de negócios; cadastro de vendas a crédito, com informações sobre a situação do pagamento e cadastro incompleto de clientes; controlo de estoque e informações de pagamento de fornecedores. Perder ou danificar os impactos das informações relevantes (talvez irreversivelmente) sobre a produtividade da empresa, sua participação no mercado e estabilidade financeira.

3. Disponibilidade: significa garantir que os dados estejam à disposição das partes interessadas, quando necessário. Não possuir este atributo fundamental pode causar: perda de negócios; danos à confiabilidade da empresa perante funcionários e clientes; redução geral no desempenho; dano irreversível à permanência da empresa no mercado; É o que afirma a empresa E-VAL Tecnología, empresa do grupo com o mesmo nome, que opera no domínio das soluções de segurança.

E-VAL Tecnología, destacando a importância de avaliar o risco inerente ao vazamento de dados, comentou que: “O vazamento de dados tem sido destaque nos principais sites e notícias nos últimos tempos. Recentemente, por exemplo, vimos um grande escândalo no Facebook. O que mais chamou nossa atenção neste vazamento foi o quão vulneráveis somos. Além disso, vimos como esse tipo de situação pode ser prejudicial para nossas vidas e também para as empresas ”.

Em relação aos riscos, esta empresa refere que estes existirão sempre, e consequentemente enumera seis “(6) acções simples capazes de mitigar o impacto deste risco, evitando que este tipo de incidente ocorra, o que se pode afirmar da seguinte forma:

1- As empresas devem considerar o investimento em segurança da informação como elemento fundamental, principalmente em um momento em que os clientes estão cada vez mais conectados e realizando transações financeiras online. Na verdade, de acordo com a empresa E-VAL Tecnología, esta etapa depende fundamentalmente da conscientização das empresas, pois elas devem entender que o roubo de dados pode envolver informações pessoais, informações pessoalmente identificáveis, segredos comerciais ou propriedade intelectual.

2- Desenhar um conjunto de acções capazes de reduzir o impacto do acesso não autorizado aos dados e mitigar os danos causados em caso de violação de dados; desenvolver um plano de resposta à violação de dados.

3- Ter uma política de segurança da informação que inclua a protecção de dados, política que consiste em incluir em seu conteúdo uma descrição de como a empresa protege seus **activos** e dados, como requisitos tecnológicos e estratégias de mudança da empresa.

4- Garantir uma equipe treinada para evitar vazamento de dados, pois o treinamento dos funcionários é garantia de segurança nos diversos níveis da empresa.

5- Adaptar uma ferramenta utilitária obrigatória capaz de garantir a segurança da informação e **protecção** eficaz dos dados.

6- Aplicar plano e políticas de resposta a vazamentos de dados capazes de atender a todas as áreas consideradas de risco, que consiste na realização de auditorias aprofundadas pelas instituições competentes, para garantir que todos os procedimentos funcionam de forma eficiente e sem margem de erro. No entanto, para muitos, o estágio de teste deve ser uma das partes mais desafiadoras, portanto, a área de segurança da informação deve sempre tentar evitar o vazamento de dados.

Fator de custo de oportunidade

A terminologia "custo de oportunidade" no uso das TIC vem ganhando forte presença mundial, principalmente em países mais desenvolvidos como Estados Unidos, Alemanha, Reino Unido, França, Japão, entre outros, e não será diferente para Angola, porque o cumprimento da legislação em vigor em matéria de protecção de dados pessoais é essencial para a prevenção de elevados custos que podem ser evitados em caso de fuga de dados, não adaptando a protecção de dados pessoais às leis aprovadas em cada país.

A decisão de adesão imediata ou futura às leis de protecção de dados é o que torna fundamental a aplicação do custo de oportunidade em TIC, uma vez que o custo de oportunidade representa o valor associado à melhor opção não escolhida, pois ao fazer uma determinada escolha, as outras possibilidades são postas de lado, porque são exclusivas (escolher uma é rejeitar outras).

Para a alternativa escolhida, o maior benefício não obtido com as possibilidades não selecionadas está associado ao "custo de oportunidade", ou seja, "a escolha de uma determinada opção impede o usufruto dos benefícios que as outras opções podem

proporcionar. O maior valor associado a benefícios não verificados pode ser entendido como um custo da opção escolhida, um custo denominado "oportunidade".

As instituições angolanas, sejam públicas, privadas ou cooperativas, não devem considerar que o cumprimento da legislação em vigor sobre protecção de dados é uma imposição do Estado angolano, nem devem pensar que constitui um obstáculo ao desenvolvimento da economia nacional. Pelo contrário, deve ser visto como uma vantagem.

João Sitta, advogado especializado em propriedade intelectual e direito digital, membro da International Association of Privacy Professionals (IAPP) e integrante da equipe de Zavagna Gralha Advogadose explica que, no Brasil, a protecção de dados está associada a notícias sobre vazamento de informações capazes de gerar grandes prejuízos para as empresas e, em particular, penalidades que podem chegar a 50 milhões ou 2% do faturamento em caso de descumprimento da legislação. Considera (Sitta, 2020) a importância de utilizar o custo de oportunidade de acordo com a lei de protecção de dados pessoais, com base em 3 pontos:

Em **primeiro** lugar, a Lei de **Protecção** de Dados coloca o proprietário no centro das **actividades** que envolvem a manipulação de seus próprios dados, e é justamente neste ponto que surge a oportunidade de considerar a privacidade do usuário como um factor diferenciador no mercado. Ao cumprir o disposto na lei, as empresas devem tratar os dados pessoais de forma aberta, transparente e responsável, o que demonstra nãoé só preocupação com as indesejáveissanções legais, mas, sobretudo, o apreço pela privacidade dos seus clientes.

Um estudo da Verint Systems Inc. em conjunto com a Opinium Research LLC mostrou que 89% dos 24.000 consumidores entrevistados acham que é importante saber como seus dados pessoais são protegidos e 84% dizem que é essencial saber se suas informações estão sendo compartilhadas com terceiros. No Brasil, pesquisa realizada por um pesquisador da Universidade Federal de Uberlândia, com 864 entrevistados, mostrou que 95,7% deles se preocupam com a privacidade na relação de consumo. Por esse motivo, a inserção da privacidade e o tratamento adequado dos dados na empresa podem representar uma importante vantagem competitiva, principalmente quando se considera a baixa adesão das empresas brasileiras.

Segundo: a Lei de Protecção de Dados representa um aumento do potencial de transações nacionais e internacionais; Isso estabelece padrões globais de protecção de dados que

ainda não existiam no Brasil e cuja ausência poderia representar (já representou) um obstáculo para os negócios com empresas estrangeiras. Por exemplo, a RGPD (Lei Europeia de Protecção de Dados) exige que as empresas do bloco apenas transfiram dados para países com níveis de protecção equivalentes aos seus.

Talvez seja justamente por uma regulamentação de dados pessoais desde 1999 que o Chile, e não o Brasil, foi escolhido pelo gigante Google para hospedar seu primeiro data center na América Latina, com um investimento de 150 milhões de dólares. No âmbito nacional, como a lei estabelece co-responsabilidade entre quem controla e quem opera os dados, a tendência é que as empresas só iniciem negócios com parceiros que demonstrem um nível adequado de conformidade. Nesta etapa, o cumprimento da legislação representa mais do que um custo, é na verdade uma oportunidade de negócio.

Em **terceiro** e último lugar, a Protecção de Dados é uma excelente oportunidade para "arrumar a casa" e organizar todos os processos e produtos que envolvem a colecta, transferência ou armazenamento de dados pessoais, sejam de clientes ou funcionários. Os requisitos aí contidos implicam necessariamente o tratamento seguro dos dados pessoais, o que atenua o risco de fuga, maliciosa ou não, e reduz as perdas a ela associadas. Um estudo anual conduzido pela IBM em conjunto com o Ponemon Institute indica que o custo médio de um vazamento para uma empresa de dados é de US $ 3,9 milhões, que pode ser reduzido para menos de um terço desse valor se for detectado dentro de 200 dias. Portanto, cumprir a lei de Protecção de Dados significa reduzir os riscos envolvidos no seu processamento.

Neste sentido, coincide plenamente com os critérios deste especialista, tendo em conta que agora nota-se cada vez maisa importância da Lei de Protecção de Dados, para as organizações que a percebem como uma oportunidade estratégica para estreitar o vínculo com o cliente , melhorar as relações comerciais e evitar os riscos inerentes e a economia da informação certamente ocupará uma posição privilegiada nos próximos anos, ao transformar custo em oportunidade e valor.

Fator de Competitividade

A competitividade tem sido objecto de estudos com diferentes abordagens. Na abordagem de competitividade de posição, discute-se a vantagem competitiva de Industrias y Naciones, Porter (1993), baseada em cinco tipos de forças competitivas: poder de clientes e fornecedores, acções competitivas, possibilidade de entrada de novos concorrentes ou produtos ou, serviços substitutos.

A competitividade é frequentemente vista no contexto da economia de mercado. Nesse sentido, competitividade empresarial significa obter retorno igual ou superior ao dos concorrentes no mercado. Se a lucratividade de uma empresa, em economia aberta, for menor que a de suas rivais, mesmo que tenha que remunerar seus trabalhadores, fornecedores e acionistas, no médio ou longo prazo ela se enfraquece até chegar a zero e virar negativa. Na verdade, a vantagem competitivabaseia-se em três pilares (Porter, 1987) para se posicionar no mercado acima dos concorrentes:

Custos: quando a empresa consegue produzir a um custo muito inferior ao de seus concorrentes (muito relevante em peças e produtos electrónica).

Diferenciação: quando a empresa oferece produtos com qualidades ou serviços únicos.

Especialização: quando a empresa se especializa em um nicho específico.

A abordagem usada para desenvolver estratégias em muitos sectores é baseada precisamente no modelo das cinco forças de análise competitiva de Porter, que explica como a intensidade da competição entre as organizações varia de um sector para outro, tendo um denominador comum que é expresso onde a intensidade da competição é maior nas indústrias de baixo lucro.

Outros autores, que se têm dedicado a desenvolver ideias e técnicas sobre a dinâmica do ambiente externo e seus impactos na competitividade das organizações, tomam o modelo de Michael Porter como ponto de partida. Essas cinco forças competitivas que definem um sector industrial são alteradas pela TI, pois podem aumentar o poder de barganha dos fornecedores ou se tornar uma barreira à entrada em um sector; O investimento em TI diminui o custo ou aumenta a diferenciação da empresa, causando uma mudança tecnológica sustentável.

Pelo exposto é evidente que a opção por novos investimentos em TI, para protecção de dados pessoais e em instituições públicas e privadas angolanas, é um diferencial competitivo e não uma despesa adicional para as mesmas.

Conclusões

1. ***Os efeitos sobre a dinâmica competitiva da implementação da tecnologia da informação nos processos de negócios aumentaram dramaticamente -desde a década de 1990-, a adopção massiva por empresas de Internet e medidas de***

protecção de software corporativo informações contra perda, roubo e vazamento de dados.

2. ***O surgimento de novas tecnologias da informação implica uma ameaça implícita à penetração de bancos de dados confidenciais de instituições públicas e privadas, incluindo pessoas físicas, gerando escândalos internacionais milionários relacionados ao vazamento de dados.***
3. ***A protecção de dados pessoais contribui significativamente para a redução de custos e pode ser utilizada como vantagem competitiva em instituições públicas e privadas, no caso específico de Angola ao cumprir a Lei da protecção de dados pessoais (Lei n.º 22 / 11, de 17 de junho).***
4. ***O ritmo alarmante que a vulnerabilidade em segurança de dados está assumindo nas instituições afectará menos as empresas com maior capacidade de prevenção e que a admitam de forma mais rápida e eficiente como vantagem competitiva.***
5. ***O monitoramento detalhado das novas tecnologias de informação e o diálogo constante com os usuários são necessários para obter vantagens competitivas.***

Referencias bibliográficas

1. Aaker, D. A. (2001). Administração estratégica de mercado. 5. ed. Porto Alegre: Bookman.
2. Barney, J. B. (2010). Gaining and sustaining competitive advantage. Upper Saddle River: NJ. Pearson/Prentice Hall, EEUU.
3. Bourdon, W. (2020) *Hacker português Rui Pinto* é a fonte do Luanda Leaks. *VOA Português*...Consultado dia 07 de Junho de 2020. Em https://www.voaportugues.com/a/hacker-portugu%C3%AAs-rui-pinto-%C3%A9-a-fonte-do-luanda-leaks-diz-seu-advogado/5261732.html
4. Cavalcanti, Marly Org. (2003).Gestão estratégica de negócios: evolução, cenários, diagnóstico e ação.São Paulo: Pioneira Thomson Learning, Brasil.
5. Hitt, M.A; Ireland, R. D; Hoskisson, R. E (2002). Administração Estratégica. São Paulo: Pioneira Thomson Learning, Brasil.
6. Hunt, Shelby D. Evolutionary economics, endogenous growth models, and resource-advantage theory. Eastern Economic Journal; Fall 1997(a); 23, 4
7. Importancia da Mitigação de Riscos operacionais. Em https://blog.sonda.com/mitigacao-de-riscos-operacionais-entenda-a-importancia/
8. Luanda Leaks - SIC Notícias (2020).Uma investigação internacional a Isabel dos Santos feita em exclusivo para *Portugal* pelo Expresso e pela SIC. Em https://sicnoticias.pt/especiais/luanda-leaks/2020-01-19-Luanda-Leaks--investigacao-na-integra.
9. Mathews, John A. A resource-based view of schumpeterian economic dynamics. Journal of Evolutionary Economics, 2002, Vol. 12 Issue 1/2, p29, 26p
10. Oliveira P. (2018). Segurança de dados avança e já é fator de competitividade. Em https://www.mundodomarketing.com.br/entrevistas/38008/seguranca-de-dados-avanca-e-ja-e-fator-de-competitividade.html,
11. Os 21 majores casos de violacao de dados (2018). Em https://epocanegocios.globo.com/Empresa/noticia/2018/12/os-21-maiores-casos-de-violacao-de-dados-de-2018.html

12. Porter, M. (1990). Vantagem competitiva: criando e sustentando um desempenho superior. Rio de Janeiro: Campus, Brasil.
13. Porter, M. (2015). Ventaja Competitiva. 2ª edición reformada, Editorial Patria, México
14. Positivo (2019). Panorama–Vazamento de dados Tudo sobre tecnologia da informação. Em https://www.meupositivo.com.br/panoramapositivo/vazamento-de-dados/
15. Proteção de dados: custo ou oportunidade? -MIGALHAS DE PESO (2020). Em https://www.migalhas.com.br/depeso/320083/protecao-de-dados-custo-ou-oportunidade.
16. Protecção de Dados Pessoais - CFA. Quadro *Legal*. Constituição da República de Angola (direito à reserva da vida privada). Lei da Proteção de Dados Pessoais (Lei n.º 22/11, de 17 de Junho). Em https://cfa.legal/wp-content/uploads/2019/03/Protec%C3%A7%C3%A3o-de-dados-pessoais.pdf.
17. Rodríguez, M.A., Ricart, J.E e Sanchez, P. Sustainable Development and the Sustainability of Competitive Advantage: A Dynamic and Sustainable View of the Firm. Creativity and innovation management, Oxford, v.11, n.3, set.2002, p 135-146.
18. Samuelson P.A., Nordhaus W.D (2005). Economia, 18ª Edição, McGraw-Hill, Madrid, 2005.