UPDATE

Digital Business Community

#75
OUTUBRO 2021

Digital Union

2ª Sessão

Soberania Digital & Cibersegurança

Que soberania queremos na Europa a 27?

Perdida a batalha da soberania tecnológica, a UE terá que saber definir o que quer ter sediado no espaço europeu em termos digitais. Com ações que envolvam todos, para garantir que ganha soberania digital. A cibersegurança é essencial neste processo, mas o novo pacote de medidas não chega para reganhar relevância.

O PAPEL DA CIBERSEGURANÇA é central no reforço da soberania digital europeia. Mas, embora estejam a ser dados passos importantes, a UE já foi ultrapassada em termos tecnológicos por outras geografias, pelo que as pessoas e os processos terão de ser agora a aposta. Há que saber gerir a proliferação e complexidade do quadro legislativo, sob pena do seu impacto nas organizações e na sua defesa contra as crescentes ameaças cibernéticas. A adoção de tecnologias modernas de segurança da informação, através do poder do hacking, é um dos caminhos, até porque está sempre tudo a mudar no mundo online e a imprevisibilidade é única constante, como ficou claro nesta 2ª sessão do ciclo 'Digital Union', uma parceria da APDC com a VdA para analisar os grandes temas do digital, que decorreu a 7 de outubro.

O tema da soberania digital, se já era debatido na Europa nos últimos anos, ganhou uma nova dimensão com a pandemia de Covid-19 e a crescente dependência das tecnologias digitais. É que a realidade veio mostrar uma crescente dependência de um diminuto grupo de empresas globais, sediadas fora do espaço comunitário, que controlo o mercado e os dados das pessoas e das organizações, começou por alertar Inês Antas de Barros, Associada Coordenadora da VdA, na sua apresentação inicial sobre o tema desta iniciativa: Soberania Digital & Cibersegurança.

Bruxelas tem a consciência da perda de controlo sobre os dados pessoais na UE, assim como da dificuldade em criar e implementar legislação, o que coloca em risco o desenvolvimento económico, já que as poucas empresas tecnológicas europeias que existem apenas operam em nichos de mercado. Acrescem as preocupações em termos do impacto social desta realidade, com o aumento do digital divide e das ameaças ambientais, e uma "crescente vulnerabilidade ao cibercrime e aos ataques", explica.

Por isso, "o legislador europeu, percebendo o que são as fraquezas da UE relativamente à

Bruxelas tem várias iniciativas já aprovadas e outras em processo de aprovação, de forma a responder à dependência excessiva de tecnologia estrangeira, ao número reduzido de fornecedores e à utilização dos dados de forma transparente

soberania digital, decidiu atuar. Há várias iniciativas já aprovadas e outras em processo de aprovação, para responder à dependência excessiva de tecnologia estrangeira, a um número reduzido de fornecedores e à utilização dos dados para diferentes finalidades e de uma forma não transparente".

Assim, além da aprovação da Estratégia Digital Europeia, foram definidas várias ações para consolidar a soberania digital: regulamento dos serviços digitais, estratégia para os dados, regulamento dos mercados digitais, estratégia industrial, conetividade, computação de alto desempenho, conetividade, competências digitais e cibersegurança. O objetivo é colocar a tecnologia ao serviço dos cidadãos, criar uma economia digital justa e competitiva e fomentar uma sociedade aberta e justa, acrescentou.

UM PAPEL CENTRAL

O papel da cibersegurança é central e Inês Antas de Barros detalha que são cinco os objetivos da UE neste âmbito. A começar pelo reforço da resiliência coletiva da Europa contra ciberameaças, assim como o reforço da liderança da UE em termos de regras e normas internacionais do ciberespaço e o aumento da confiança dos cidadãos e empresas nos serviços e ferramentas digitais. A promoção de um ciberespaço à escala mundial aberto, estável e seguro e o reforço da soberania tecnológica também são metas para todos os estados-membros.

Inês Antas de Barros

Associada Coordenadora, VdA

"O tema da soberania digital ganhou relevância com a pandemia, com a crescente dependência do digital e de um pequeno número de grandes tecnológicas, que controlam o mercado e os dados pessoais. O legislador percebeu as fraquezas da UE e decidiu atuar"

"Há estratégias definidas em múltiplas áreas se alcançarem os objetivos definidos por Bruxelas. A cibersegurança é uma delas, para reforçar a resiliência europeia, liderança nas regras internacionais do ciberespaço, confiança dos cidadãos, promoção do ciberespaço e a soberania tecnológica"

"O tema da cibersegurança está na ordem o dia e na agenda do regulador europeu. As organizações têm de estar atentas e mapear as diferentes obrigações. É essencial adotar uma estratégia holística que enderece as diferentes componentes: tecnológica, jurídica e de negócio/ operacional, tendo em conta o aumento das ameaças a nível mundial"

António José Gameiro Marques

Diretor Geral, GNS

"Pessoas, processos e tecnologia são as dimensões do digital. A UE está a correr atrás do prejuízo, a endereçar pessoas e processos, porque já não consegue agarrar os temas ligados à tecnologia. Felizmente acordou e tem um plano de ação para o digital, mas está tudo centrado na regulamentação"

"A Europa não pode tentar reganhar a soberania fazendo coisas que outros já fazem melhor. É uma perda de tempo. Tem de saber identificar o que é essencial ter, na componente tecnológica. Com uma visão. Aprendemos alguma coisa, vamos ver é se é consequente"

"O 5G vem abrir um conjunto de oportunidades, pelas suas características técnicas intrínsecas. Nunca uma alteração tecnológica deste género teve à cabeça uma preocupação de cibersegurança tão grande. Só posso estar confiante no resultado"

No mercado nacional, existe já múltiplas iniciativas que respondem aos objetivos de Bruxelas, com legislação nacional (como a Diretiva de Segurança e Redes de informação, o recente decreto-lei 65/2021 que estabelece o regime jurídico da segurança do ciberespaço ou o decreto-lei das infraestruturas críticas), que é complementada por regulação setorial.

Mas há ainda um conjunto de iniciativas europeias que vão ter impactos em Portugal. Como adianta a oradora, a proposta da CE de revisão da Diretiva NIS virá alargar o escopo de aplicação e as obrigações para as organizações, assim como a proposta de uma nova diretiva sobre a resiliência das entidades críticas e outras iniciativas, como a toolbox sobre a cibersegurança no 5G. É que entre as alterações propostas estão o alargamento dos setores abrangidos, a eliminação da distinção entre operadores de serviços essenciais e serviços digitais, a definição de mais requisitos de segurança ou a criação de regras de supervisão mais estritas.

"A cibersegurança está na ordem do dia e na agenda regulatória europeia. As organizações têm que estar atentas e mapear as diferentes obrigações, porque há muita legislação dispersa. A sua preparação é para este novo pacote legislativo é essencial. Terão de ter uma estratégia holística de cibersegurança que aborde as diferentes componentes – tecnológica, jurídica e de negócio/operacional – porque o tema está para ficar, com o aumento das ameaças ao nível mundial", conclui.

DESAFIO DE GERIR A COMPLEXIDADE

Já no período de debate, moderado por Sandra Fazenda Almeida, Diretora Executiva da APDC, e por Tiago Bessa, Partner da VdA, foi dada a visão dos vários stakeholders do mercado nacional. A começar pelo diretor geral do Gabinete Nacional de Segurança (GNS), no âmbito do qual funciona o Centro Nacional de Cibersegurança (CNCS), que comemora precisamente 7 anos de atividade. António Gameiro Marques começa por destacar que "soberania digital é muito mais que cibersegurança. Se atacarmos os problemas de cibersegurança no espaço europeu não resolvemos o problema de soberania. Nada disso".

Para este responsável, as "pessoas, processos e tecnologia são as dimensões do digital e a UE está a correr atrás do prejuízo. Está a endereçar as dimensões pessoas e processos, porque já não consegue agarrar os temas ligados à tecnologia". Assim, explica que a estrutura tecnologia utilizada na Europa assenta sobretudo em dois gigantes tecnológicos, um norte-americano e outro chinês, e os dispositivos que usamos são concebidos nos EUA e China e fabricados na China e Taiwan.

Também os sistemas operativos, o "coração de qualquer dispositivo digital", são "predominantemente norte-americanos", tal como os browsers e sistemas usados, como as redes sociais, que são "coletores impressionantes de informação sobre nós todos". Esta total dependência ficou bem demonstrada pelo recente apagão do Facebook, acrescenta.

Para o diretor geral do GNS, "a Europa felizmente acordou com esta presidente da CE, que tem no seu plano de ação desenvolver a componente digital. Mas vai desenvolvê-la centrando-se na regulamentação". Assim, defende que "o que se pode debater é onde nos poderemos

André Baptista

Security researcher and bug bounty hunter; Professor at University of Porto; Founder & CTO at PENTHACK

"Em 2020 fomos invadidos pela era digital e há uma dependência clara dos processos tecnológicos. Temos que saber desligar. Às vezes é preciso fazer um reset e ver quais os efeitos da utilização massiva de tecnologia"

"Será que dependemos das redes e das tecnologias e somos controlados por elas? As tecnologias facilitam a nossa vida, tornam tudo mais fácil, mas serão uma ameaça?

A internet está em desenvolvimento e os seus efeitos sociais são imprevisíveis. Conseguiremos ter liberdade e soberania digital a mesmo tempo? Espero que sim"

"Apesar das empresas terem planos de backup e implementações de segurança, há hackers como motivação. Uma das soluções que complementam esta defesa é o ataque, tentando encontrar vulnerabilidades complexas de explorar, com o talento qualificado para isso"

Paulo Moniz

Information Security & IT Risk, EDP

"Todos os sistemas que funcionam à nossa volta estão impregnados de tecnologia, que é cada vez mais commodity vulnerável. No mundo digital, por muitos esforços que existam, só a atuação das entidades não é suficiente para defender a nossa soberania. Num conceito de guerra digital, um ataque pode ser feito até por uma pen"

"Awareness, comunicação e resiliência são fundamentais num ataque informático. Quando nos acontece, ficamos muito mais alertas para tudo"

"Qualquer operador tem que ter planos de segurança, para garantir continuidade do negócio. É certo que os backups são cada vez mais tecnológicos e também eles são atacáveis. Mas a ideia é ter resiliência: quando a organização sofre um impacto, seja digital ou não, tem que ter um plano de emergência e de continuidade de negócio. Nunca pode ser esquecido"

---

centrar para recuperar alguma soberania, que será precisamente nos dados, incluindo os metadados sobre nos próprios. Não podemos deixar que continuem a ser guardados fora do território europeu. A soberania digital que não está perdida, mas está muito debilitada".

Reiterando as afirmações de António Gameiro Marques, Paulo Moniz, Information Security & IT Risk da EDP não tem dúvidas de que, cada vez mais, todas as infraestruturas e sistemas que funcionam à nossa volta estão "impregnados de tecnologia, ela própria cada vez mais uma commodity vulnerável aos riscos digitais".

"No mundo digital, nas infraestruturas controladas digitalmente, por muitos esforços que se façam, só a atuação das entidades não é suficiente para defender a nossa soberania. Acho que isso está a ficar claro com a legislação europeia. Num conceito de guerra digital e de um ataque à nossa soberania por via digital, a defesa não pode ser só feita pelo que conhecemos no mundo convencional. É que um ataque pode vir até de uma pen", considera, pelo que além da regulação, há que ter a certeza de que "as organizações asseguram a segurança do seu negócio, mas também da sociedade como um todo".

DEFINIR O QUE É ESSENCIAL

Já André Baptista, security researcher and bug bounty hunter, professor da Universidade do Porto e fundador e CTO da startup PENTHACK, centrada em serviços de cibersegurança disruptivos e inovadores, mostra-se muito preocupado com os impactos do digital na vida das pessoas, sobretudo nas faixas etárias mais novas.

"Esta era digital em que vivemos teve início no ano passado, com a pandemia e a com a invasão e dependência clara dos processos tecnológicos. Não era uma realidade nova, mas claramente acelerou. Entrar o digital tem sido um mergulho, mas Temos de saber desligar e parar. Às vezes é preciso fazer um reset", alerta.

Destacando o apagão das plataformas do Facebook, que "veio demonstrar e colocar várias questões. Será que dependemos das redes e das tecnologias e somos controlados por elas?", considera que "temos que ver os efeitos da utilização massiva da tecnologia. Ela facilita a nossa vida, torna tudo mais fácil e rápido, mas será já uma ameaça à liberdade?"

Apesar da CE ter vindo a desenvolver um conjunto de iniciativas na área de cibersegurança, o facto é que "os ataques têm vindo a tornar-se cada vez mais frequentes e sofisticados, com efeitos devastadores a nível pessoal e coletivo". Por isso, o caminho terá que passar, nomeadamente, por colocar os hackers a defender a Europa, com "tecnologias modernas de segurança da informação, através do poder do hacking. A internet está em desenvolvimento e os efeitos sociais são imprevisíveis. Conseguimos ter liberdade ou soberania digital a mesmo tempo? Espero que sim", remata.

Questionado sobre se a Europa ainda tem espaço para ganhar algum do tempo perdido no que respeita à soberania tecnológica mundial, o líder do GNS considera que "não poderá tentar reganhar a soberania fazendo coisas que outros já fazem melhor". Sendo a UE um "grande espaço económico onde a centralidade do ser humano releva em relação aos outros", defende que há que definir o que é essencial que esteja sediado na Europa no domínio digital.

"Temos que fazer este pensamento conjunto, porque só assim é que efetivamente teremos algo a dizer nas três dimensões do digital, sobretudo na tecnológica. Aprendemos alguma coisa, agora vamos ver se somos consequentes e de transformamos isso em ações o nível europeu ou se cada estado-membro trata da sua vida separadamente. Era o que esperaria que acontecesse", acrescenta.

Awareness, comunicação e resiliência foram as grandes aprendizagens retiradas pela EDP no ataque informático de que foi alvo em abril do ano passado. Paulo Moniz explica que a detentora de uma infraestrutura crítica nacional tem a "obrigação e o dever de aproveitar a situação para construir coisas melhores. O ataque criou awareness, pois ficámos muito mais alerta, quando acontece alguma coisa. Os efeitos criaram urgência e premência e consciencialização dentro da organização".

Fator essencial é também, na sua ótica, a comunicação. "Todos temos um meio de comunicação nas nossas mãos e é muito natural haver descontrolo da informação que sai, gerando-se uma onda que provoca reações, nomeadamente de receio nos stakeholders", pelo que há que, através dos canais de comunicação com todas as entidades, fazer uma informação correta, não deixando que esta se propague de forma descontrolada. Finalmente, na resiliência, "qualquer operador tem que ter planos de segurança, para ter continuidade do negócio".

CENTRAR E CONJUGAR ESFORÇOS

Mas, apesar das empresas terem planos de backup, há um conjunto de vulnerabilidades que continuam a ser detetadas. É que, "com motivação, os hackers podem sempre entrar nas organizações, mesmo aquelas que implementam soluções defensivas", garante André Baptista. Uma das soluções para complementar esta defesa passa pelo ataque, com o recurso ao hacking para "tentar encontrar vulnerabilidades complexas de explorar" e, dessa forma, as prevenir.

E garante que Portugal tem talento, como ficou provado no recente European Cybersecurity Challenge 2021, organizado pela ENISA, onde a equipa nacional ficou na 7ª posição entre 19 países concorrentes. O problema é que os melhores continuam a sair do país para grandes grupos internacionais. "Precisamos de investir à séria na educação e na formação e as nossas organizações têm que conseguir oferecer competitividade de mercado, evitando que as pessoas saiam do país, porque são necessárias em termos de defesa. Há já exemplos de países que criaram unidades de defesa ofensiva e a Europa e Portugal têm que investir nesta área", remata.

Um dos temas abordados foi a certificação em cibersegurança, com duas frentes a serem trabalhadas: a certificação de conformidade com o Quadro Nacional de Referência em Cibersegurança e o selo digital, uma medida prioritária do Portugal Digital. António Gameiro Marques diz que o CNCS tem neste momento tudo o que é necessário para desenvolver a framework e criar as entidades que vão fazer a acreditação, assegurando ainda o respetivo financiamento, não só para criar todo o processo, mas também para ajudar as empresas.

Mas Paulo Moniz deixa claro que "uma orienta-

ção puramente por compliance pode não representar uma segurança. O tema da certificação tem esta nuance, do lado mais negro do cenário". Terá assim de ser uma certificação "orientada ao risco, sob pena de se poder ter uma falsa sensação de segurança". Mas ajuda claramente "num processo de supply chain. Temos uma cadeia de valor imensa, que é um aspeto crucial em cibersegurança. O facto de ter este processo mais facilitado na triagem aos fornecedores dá muito mais confiança às organizações e à sociedade. Será uma certificação muito bem-vinda, se for bem feita", remata.

Também André Baptista diz que as "certificações, por si só, não serão suficientes para conseguir garantir a segurança. É completamente impossível estamos 100% seguros. Há sempre vulnerabilidades a surgir porque se trata do jogo do gato e do rato. É uma questão de colocar esforços e minimizar a probabilidade de se sofrerem ataques. E, ainda assim, podemos sempre ser atacados, como o mostra o recente caso do Twitch".

Sobre a segurança das redes 5G, uma preocupação que levou até Bruxelas a apresentar uma toolbox, António Gameiro Marques deixa claro que o 5G se trata de um "assunto fundamentalmente do regulador Anacom". Ainda assim, o CNCS trabalhou no desenvolvimento de um primeiro estudo de risco para aprofundar o tema e contribuir para a toolbox da CE, produzindo um conjunto de recomendações que foram entregues às tutelas.

Uma delas foi a de que o Conselho de Segurança do Ciberespaço se deverá pronunciar sobre as grandes opções tecnológicas das soluções 5G a colocar em Portugal. E relembra que "há que estar em alinhamento com as orientações de Bruxelas. Todos sabemos que a questão mais importante do 5G não é tecnológica, mas sim geoestratégica".•

>>>> **Aceda ao vídeo do Evento**
https://youtu.be/9e9KZSbjTaA

Patrocinadores Silver

accenture altice BOLD by devoteam Capgemini engineering
ERICSSON HUAWEI NOKIA NOS vodafone

Parceiros para o Talento

AON Empower Results®
the key talent

Patrocinadores Bronze

AXIANS CISCO DELOITTE DXC TECHNOLOGY GOOGLE
HP HPE IBM INETUM MICROSOFT MINSAIT SAP SAS

Parceiros

NOSSA VIATECLA VdA