Publicado no Jornal i Online no dia 29/08/2018

OBSERVATÓRIO CONTRA A FRAUDE

Nas Malhas do Crime Informático

As tecnologias não se restringem apenas ao clique de um telemóvel/tablet/computador, este "simples" clique poderá ter consequências nefastas (cibercrime) para os indivíduos, em particular, e para a sociedade, em geral.

Silvério Cordeiro

Anthony Giddens define no livro "O Mundo na Era da Globalização" o conceito de globalização como a intensificação das relações sociais em escala mundial e as conexões entre as diferentes regiões do globo, através das quais os acontecimentos locais sofrem influência dos acontecimentos que ocorrem a milhas de distância. As consequências dos nossos atos repercutem-se assim em espaços e tempos distantes - interconexões globais e locais. A globalização é política, tecnológica e cultural, além de económica, sendo influenciada pelo progresso dos sistemas de comunicação.

As tecnologias têm influenciado a vida do ser humano, exigindo uma preocupação acrescida com as mudanças culturais, sociais, políticas e económicas. As tecnologias não se restringem apenas ao clique de um telemóvel/tablet/computador, este "simples" clique poderá ter consequências nefastas (cibercrime) para os indivíduos, em particular, e para a sociedade, em geral.

O cibercrime corresponde aos crimes cibernéticos que envolvam qualquer atividade ou prática ilícita realizados a partir de dispositivos eletrónicos, nomeadamente computadores, e frequentemente com recurso à Internet.

Desta forma, é premente a necessidade dos governos, organizações não-governamentais e sociedade repensarem estes fenómenos, onde novos desafios são colocados pela própria transformação que a inovação e produção de conteúdos da realidade digital está a provocar.

Torna-se assim imprescindível sensibilizar a visão que a comunidade tem dos comportamentos associados ao cibercrime, desenvolvendo no terreno medidas de proteção/precaução, e verificar quais os casos de sucesso noutros países e replicá-los. Tal como aconteceu em 2009 com a génese da lei que o Estado criou para controlar e fiscalizar tais fenómenos - Lei n.º 109/2009 de 15 de setembro. Estas práticas compreendem invasões de sistema, disseminação de vírus, roubo de identidade, acesso a informações confidenciais, entre outras.

O conceito tem uma predominância transnacional e está diretamente relacionado com o simples aumento de computadores pessoais, permitindo a execução de práticas criminosas de qualquer parte do planeta e a partir do conforto das suas casas.

A diversidade dos cibercrimes praticados é ampla, o que acaba por dificultar a punição dos criminosos, por falta de leis aplicáveis. Assim, poderemos destacar como crimes cibernéticos os seguintes: pornografia infantil; lavagem de dinheiro; ciberterrorismo (ações premeditadas com motivações políticas cometidas, geralmente contra os governos, partidos e instituições governamentais); ciberativismo (envolve roubo de informações e manipulações contra organizações divulgando-as ao público e à imprensa); e o roubo (de identidade; espionagem; fraude; plágio, etc.).

Estudos revelam que, por exemplo, o crime económico tem aumentado substancialmente devido ao cibercrime, logo há uma necessidade que se tem mantido constante e está relacionada com a criação de mais recursos, por exemplo, a criação da Unidade Nacional de Combate ao Cibercrime e a Criminalidade Tecnológica (UNC3T).

Os métodos de cibercrime são variados e a comunidade ainda não se encontra totalmente sensibilizada, sobretudo na amostra populacional que apresenta uma faixa etária mais envelhecida e com pouca formação nas áreas tecnológicas. A burla informática está à nossa porta através de um simples clique no botão errado.

A título exemplificativo, os ataques de *phishing* (páginas que aparentam ser de uma fonte confiável com o único objetivo de obterem os nossos dados pessoais e secretos) apresentam ainda hoje uma grande expressão mundial, sendo exemplo o caso "Cartas da Nigéria" que consistiu em mensagens através do e-mail sobre propostas de negócio. Assim, os especialistas referem a necessidade de criar indicações de proteção aquando da navegação na internet, evitando procurar sites pouco conhecidos ou duvidosos.

Com efeito, o cibercrime é incerto e não persegue sempre os mesmos objetivos nem recorre sempre à mesma estratégia. O mundo terá de enfrentar este desafio através de um maior investimento na educação/prevenção, na administração de riscos, na cooperação internacional e na construção de habilidades jurídicas capazes de cobrir a diversidade desta criminalidade.

OBEGEF
Observatório de Economia e Gestão de Fraude