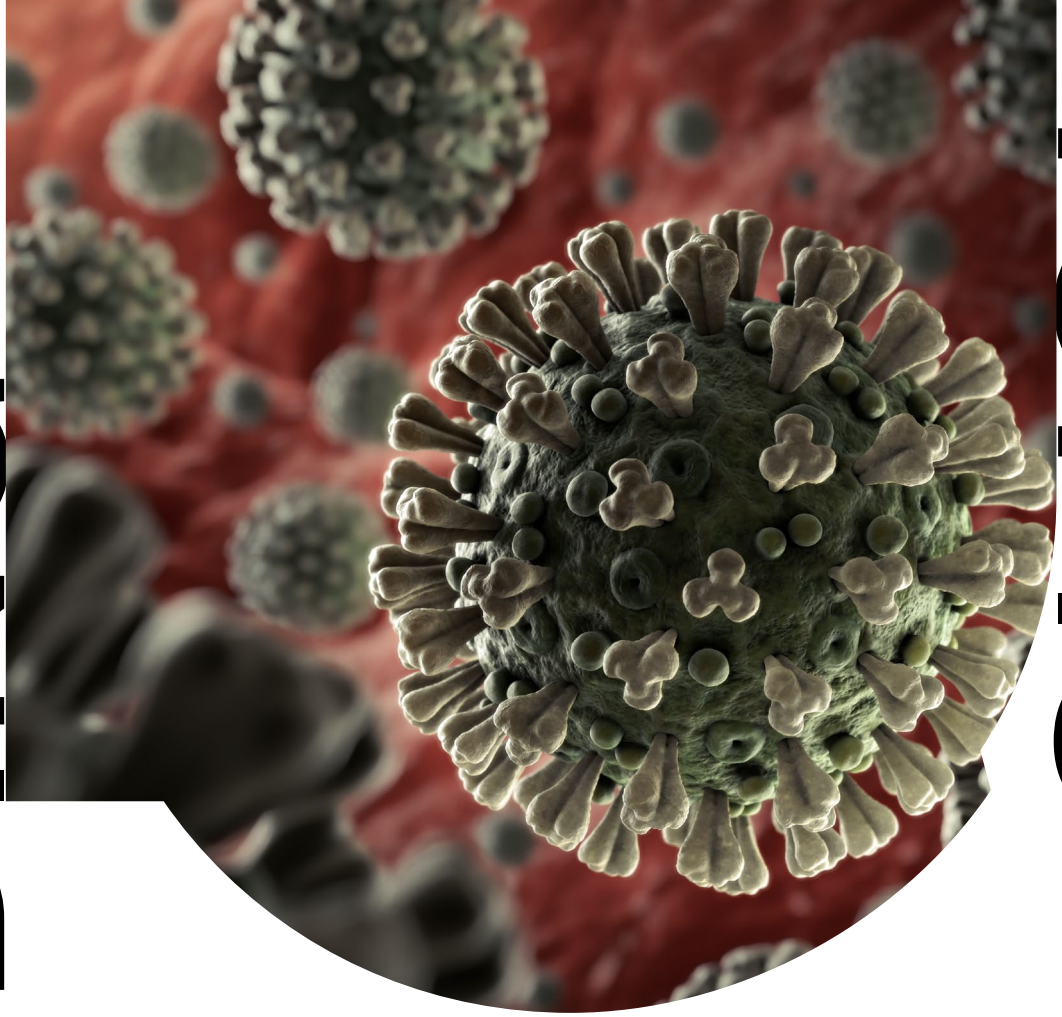
TRENDING TOPIC



06 ABR. 20

CRIMINAL, CONTRAORDENACIONAL E COMPLIANCE

Coronavírus: Cibercrime em tempo de pandemia

A opção pelo teletrabalho, incentivada pelo Governo e hoje adotada por grande parte das empresas e trabalhadores cujas atividades o permitem, obriga-nos a uma atenção redobrada aos fenómenos relacionados com o cibercrime.

PLMJ

Alexandra Mota Gomes
José Maria Formosinho Sanchez
Leonor Vasconcellos

Os tempos que vivemos obrigam-nos a desafiar o nosso estilo de vida e o dia-a-dia profissional.

Com as mudanças que nos vimos forçados a implementar surgem novos perigos e intensificam-se os do passado.

Face à distância social aumentam os contactos e comunicações através de meios eletrónicos e como consequência encontramo-nos mais vulneráveis a ataques de natureza cibernética. Assim, importa relembrar alguns dos crimes mais comuns neste contexto e os cuidados a adotar por forma a evitar ser vítima destas práticas.

"A opção pelo teletrabalho, incentivada pelo Governo e hoje largamente adotada, obriga-nos a uma atenção redobrada aos fenómenos relacionados com o cibercrime."

1. Burla informática e nas comunicações

Previsto e punido pelo artigo 221.º do Código Penal, o crime de burla informática e nas comunicações é suscetível de ser cometido por quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, interferindo no resultado de tratamento de dados ou mediante estruturação incorrecta de programa informático, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, ou usando programas, dispositivos electrónicos ou outros meios que, separadamente ou em conjunto, se destinem a diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações, é punido com pena de prisão até 3 anos ou com pena de multa. Em função do valor do prejuízo patrimonial causado, a pena poderá ser de 600 dias de multa ou até 5 anos de prisão, ou ainda de entre 2 a 8 anos de prisão.

2. Falsidade informática

O crime de falsidade informática está previsto no artigo 3.º da Lei n.º 109/2009, de 15 de setembro ("Lei do Cibercrime") e pune com uma pena até 5 anos de prisão, ou com uma pena de multa de 120 a 600 dias, quem, com intenção de provocar erro ou engano, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir no seu tratamento, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados como se o fossem.

Caso estejam em causa dados registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, o agente é punido com pena de 1 a 5 anos de prisão.

Acesso ilegítimo

O crime de acesso ilegítimo está previsto pelo artigo 6.º da Lei do Cibercrime e pune com pena de prisão até 1 ano ou com pena de multa até 120 dias, quem, sem permissão legal ou sem estar autorizado pelo proprietário, aceder a um sistema informático.

Se o acesso for conseguido através de violação de regras de segurança, o agente é punido, com pena de prisão até 3 anos ou multa.

PLMJ

E caso, através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei, ou tiver obtido benefício ou vantagem patrimonial de valor consideravelmente elevado, o agente é punido com pena de prisão de 1 a 5 anos.

3. Interceção ilegítima

O crime de interceção ilegítima, previsto pelo artigo 7.º da Lei do Cibercrime, pune com pena de prisão até 3 anos ou com pena de multa, quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele e, através de meios técnicos, interceptar transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinadas ou dele provenientes.

4. Devassa da vida privada

Previsto e punido pelo artigo 192.º do Código Penal, o crime de devassa da vida privada é suscetível de ser cometido por quem, sem consentimento e com intenção de devassar a vida privada das pessoas, designadamente a intimidade da vida familiar ou sexual:

- Intercetar, gravar, registar, utilizar, transmitir ou divulgar conversa, comunicação telefónica, mensagens de correio eletrónico ou faturação detalhada;
- Captar, fotografar, filmar, registar ou divulgar imagem das pessoas ou de objetos ou espaços íntimos;
- Observar ou escutar às ocultas pessoas que se encontrem em lugar privado; ou
- Divulgar factos relativos à vida privada ou a doença grave de outra pessoa;

É punível com pena de prisão até 1 ano ou com pena de multa até 240 dias.

5. Violação de correspondência ou de telecomunicações

O crime de violação de correspondência ou de telecomunicações, previsto no artigo 194.º do Código Penal, pune com pena até 1 ano de prisão ou pena de multa até 140 dias quem, sem consentimento, abrir encomenda, carta ou qualquer outro escrito que se encontre fechado e lhe não seja dirigido, ou tomar conhecimento, por processos técnicos, do seu conteúdo, ou impedir, por qualquer modo, que seja recebido pelo destinatário, assim como quem se intrometer no conteúdo de telecomunicações ou dele tomar conhecimento.

> **"Deve privilegiar-se a informação obtida através de fontes oficiais e plataformas seguras, não fornecendo dados pessoais através de questionários *on-line*, nem abrindo hiperligações de fontes que não possam considerar-se fidedignas."**

6. Acesso indevido

O crime de acesso indevido encontra-se previsto no artigo 47.º da Lei 58/2019, de 8 de agosto ("Lei da Proteção de Dados Pessoais"), e pune com pena de prisão até 1 ano ou com pena de multa até 120 dias quem, sem a devida autorização ou justificação, aceder, por qualquer modo, a dados pessoais.

Esta pena é agravada para o dobro quando se tratar de determinadas categorias de dados pessoais (relacionados com condenações penais, convicções políticas, dados genéticos, entre outros), quando o acesso for conseguido através de violação de regras técnicas ou de segurança, ou quando tiver proporcionado ao agente ou a terceiros benefício ou vantagem patrimonial.

Em aproveitamento da crescente ansiedade e procura de informação acerca da COVID-19, são vários os esquemas criminosos que têm surgido, particularmente por via eletrónica e informática. Foi inclusivamente feito um alerta pela INTERPOL, no passado dia 13 de março, dando nota de operações fraudulentas de burla informática e falsidade informática ("*phishing*") em temas relacionados com a COVID-19, com o objetivo de falsear comunicações eletrónicas em nome de autoridades de saúde.

Também a Polícia Judiciária emitiu um comunicado, no passado dia 17, alertando para as ciberameaças e denunciando variados esquemas fraudulentos. Alguns exemplos são a divulgação de SMS garantindo alegados reembolsos pelo governo de custos com vacinas contra a COVID-19, mediante o pagamento de uma quantia, a divulgação de mapas interativos com informação sobre a pandemia, que se destinam a infetar os equipamentos com *malware*, e campanhas de "*phishing*" orientadas para a captação de dados pessoais utilizando a imagem de entidades oficiais de saúde.

"Importa relembrar alguns dos crimes mais comuns: (i) burla informática e nas comunicações; (ii) falsidade informática; (iii) acesso ilegítimo, (iv) interceção ilegítima; (v) devassa da vida privada; (vi) violação de correspondência ou de telecomunicações; e (vii) acesso indevido."

Assim, importa ter alguns cuidados adicionais na partilha de conteúdos digitais associados à temática da COVID-19. Deve privilegiar-se a informação obtida através de fontes oficiais e plataformas seguras, não fornecendo dados pessoais através de questionários *on-line*, nem abrindo hiperligações de fontes que não possam considerar-se fidedignas, independentemente e se apresentarem como tal. ■