OS CRIMES INFORMÁTICOS NO DIREITO PENAL ANGOLANO.[1]

Jelssimi Moisés da Cunha[2]

Resumo

O presente artigo versa sobre a problemática dos crimes informáticos no Direito Penal angolano. É ponto assente de que os crimes informáticos podem definir-se em sentido amplo como aqueles em que os sistemas de tratamento automático de dados e de informação são objecto ou instrumento do crime, ou este está de forma significativa ligado à utilização desses sistemas, e que a sua evolução normativa ao nível da criminalidade informática começou no início dos anos 70 visando essencialmente a protecção da vida privada para fazer face às novas possibilidades de recolha, transmissão e armazenamento de dados possibilitada pela informática.

Importa realçar que nos crimes informáticos não se protege qualquer bem jurídico novo, nem sequer algum bem jurídico especificamente informático, e que tal, como por exemplo, nos crimes de falsidade de documentos tradicional, o bem protegido é a segurança e fiabilidade de documentos e a protecção contra o engano nas relações jurídicas, ou a veracidade na reconstituição das relações jurídicas de forma exactamente igual aos interesses protegidos pelo direito penal clássico relativamente às outras falsidades. A única especificidade deste tipo consiste no *modus operandi* onde releva a execução pelo meio informático

Neste sentido, o novo código penal angolano estabelece como crimes informáticos a falsidade informática, crime de dano informático, crime de burla informática, dentre outros.

Palavras chave: Crimes informáticos, novo código penal angolano, bem jurídico.

[1] Artigo para Revista Jurídica JuLaw (www.julaw.co.ao)
[2] Advogado.

Introdução

Vírus, spyware, worms hackers, spam... são as novas expresses reveladoras não só de uma nova forma de cultura e de ver o mundo, mas sobretudo de novas formas de ofensa aos bens jurídicos tradicionais, e talvez até a novos bens jurídicosoriundos deste novo mundo informático.

O presente estudo pretende uma visão geral sobre os crimes informáticos entre nós e sobre a consagração destas novas realidades no direito penal angolano.

No entanto, a informática perpassa já toda a nossa existência, e como tal, perpassa igualmente todos os aspectos da ciência criminal, o que torna impossível tratar todos os seus aspectos num artigo desta naturesa, com as limitações formais a ele inerente.

Com efeito, este estudo consubstancia-se num enquadramento geral de alguns tipos numa perspectiva substantiva virada para as condutas punidas, os bens jurídicos em causa nestes crimes e a relação entre eles, com algumas considerações pontuais sobre certos aspectos previstos no novo Código Penal angolano.

O presente estudo tem como objectivo apontar a eficácia da incriminação dos crimes informáticos no novo Código Penal angolano, bem como descrever as envolventes dos crimes informáticos, analisando os dispositivos legais sobre os crimes informáticos constantes no citado diploma legal.

A nossa pesquisa é do tipo bibliográfico/comparativo, dado que iremos analisar e descrever o tema em estudos a partir de obras publicadas. Assim, de acordo aos nossos objectivos, adoptamos como método de investigação os teóricos: o histórico-lógico e análise-síntese.

1. Noção e Tipologia

GARCIA MARQUES e LOURENÇO MARTINS, alertam para inexistência de um conceito de "criminalidade informática" expressamente consagrado na legislação, ou uniformemente sedimentado na doutrina e jurisprudência.

Por outro lado, "é frequente encarar a criminalidade informática como todo o acto em que o computador serve de meio para atingir um objecto criminoso ou em que o computador é o alvo simbólico desse acto ou em que o computador é o objecto do

crime". Esta "definição" levanta as principais dicotonomias que dificultam a consagração de um conceito uniforme de criminalidade informática.

De facto tem sido integrado no fenómeno da criminalidade associada às tecnologias da informação e comunicação uma série de comportamentos violadores de valores fundamentais de natureza distinta. Nestes, podemos distinguir aqueles em que a informática é apenas um meio para a prática do crime, outros em que a informática aparece como um elemento do tipo legal criminalmente punido.

Em sentido amplo, a criminalidade informática engloba toda a panóplia de actividade criminosa que pode ser levada a cabo por meios informáticos, ainda que estes não sejam mais que um instrumento para a sua prática, mas que não integra o seu tipo legal, pelo que o mesmo crime poderá ser praticado por recurso a outros meios. Em sentido estrito, entendemos nós que a criminalidade informática abarcará apenas aqueles crimes em que o elemento digital surge como parte integrador do tipo legal ou mesmo como seu objecto de protecção.

BENJAMIM SILVA RODRIGUES[3], opta por uma distinção diferente, referindo-se a «crime informático-digital próprio ou "puro"» e «crime informático-digital impróprio ou "impuro"». Refere este autor que quando aludimos à criminalidade informática-digital em sentido próprio" ou "puro", como já o deixamos entender, pretendemos identificar os tipos legais de crime em que estamos perante condutas jurídico-penalmente relevantes porque lesivas dos fluxos informacionais e comunicacionais e informático-digital, contidos/estruturantes ou veiculados/comunicados, a partir dos computadores, sistemas, redes informáticas e redes de comunicações eletrônicas publicamente acessíveis ou não, em círculos abertos ou fechados (intranet ou internet), praticados com o recurso a meios informático-digitais, enquanto "informação-informaçao", "informação-comunicaçao" ou informação-ferramenta"».

Por último, na categoria de " criminalidade informática-digital em sentido próprio", este autor inclui apenas os crimes onde o bem jurídico protegido é informático.

Como vimos supra, em sentido ligeiramente divergente, nós incluiremos na categoria de criminalidade informática em sentido estrito aqueles em que a informática

[3] Cfr. BENJAMIM SILVA RODRIGUES, Direito penal – parte especial, Tomol – Direito Penal informático-Digital, Coimbra Editora, Coimbra, 2009, P. 279.

faça parte dos seus elementos tipificadores, ainda que o bem jurídico protegido não seja digital.[4]

Os crimes informáticos podem definir-se em sentido amplo como aqueles em que os sistemas de tratamento automático de dados e de informação são objecto ou instrumento do crime, ou este está de forma significativa ligado à utilização desses sistemas.[5]

2. Evolução Histórica

A evolução normativa ao nível da criminalidade informática começou no início dos anos 70 visando essencialmente a protecção da vida privada para fazer face às novas possibilidades de recolha, transmissão e armazenamento de dados possibilitada pela informática. Apesar de esta intervenção ter como objectivo a protecção de dados pessoais, constituiu já uma indicação no sentido da criação legislativa destinada a proteger outros interesses ligados a computadores e ao tratamento informático de dados. Posteriormente, nos anos 80, pretendeu-se o combate à criminalidade económica praticada através da informática, ponto de onde se evoluiu para uma fase de salvaguarda da propriedade intelectual, fazendo face à ameaça da pirataria. Uma quarta fase tem tomado em atenção os aspectos processuais penais e a investigação deste tipo de crime. Actualmente tem-se defendido uma "quinta vaga" virada para o direito internacional e cooperação nestas matérias.[6]

3. A Sociedade da Informação

A evolução técnica e social, hodiernamente faz-se em grande parte devido à grande facilidade e rapidez na comunicação. E neste aspecto particular o uso do computador teve uma extrema importância, até um ponto em que todos os aspectos da

[4] Sobre o conceito de criminalidade informática e respectiva tipologia, alem dos autores já citados, leia-se também: João Carlos Cruz Barbosa de Macedo, "Algumas considerações acerca dos crimes informáticos em Portugal".
[5] Cfr. José António Lopes Rocha, «Criminalidade Informática: modos de execução», Pág 173
[6] *Ibdem.*

nossa vida se encontram directa ou indirectamente ligados ao uso de um computador, ou de uma rede ou sistema informático ou de tratamento automático de dados.

Na verdade, em todos os aspectos do nosso quotidiano, em todas as áreas da sociedade, tudo está computarizado, ou, melhor dizendo, automatizado. A nossa conta bancária não é mais do que um conjunto de dados informáticos, as nossas declarações de imposto são agora entregues electronicamente, praticamente todos os empregos (ou pelo menos aqueles cuja a actividade está relacionada com um escritório) exigem o domínio de computadores e são exercidos através de um.

Pode dizer-se que quase toda a gente utiliza computadores, *smarts fone* ou *tablets* diariamente, aproveitando a grande capacidade de armazenamento em pouco espaço, a rapidez e facilidade de tratamento de dados etc.

Na verdade, pode dizer-se que hodiernamente a informática[7] ocupa nos nossos dias um papel tão relevante como a escrita ou a imprensa veio ocupar após Gutemberg.

Outra evolução importante depois da criação do computador, ou em consequência desta, aconteceu com o advento e propagação da *Internet* [8], e com a consequente possibilidade de comunicação e transferência de dados e informação em tempo real, para todo o mundo e sob o manto do anonimato. Foi de tal modo importante que se pode dizer que "a introdução da internet na vida quotidiana foi uma revolução mais vertiginosa que a do automóvel, a da lámpada, da rádio, a do frigorífico, a da televisão ou a dos telefones celulares. Com o surgimento da pandemia causada pelo Coronavírus (COVID 19), os habitantes do mundo estão tão perto, á distância de um clique", e nunca como hoje a informação circulou tão livre e rapidamente, como as consequências positivas e negativas daí resultantes, de tal forma que hoje em dia são correntes as expressões "Segunda Revolução Industrial", "Sociedade da Informação" Ou "Aldeia Global"[9].

[7] Esta expressão teve origem em 1962, é da autoria de Philipe Dreyfus, que resulta da fusão das expressões *information* e *automatique*, e é um neologismo aplicável ao conjunto de disciplinas e técnicas estudadas para o tratamento automático da informação. (Cfr. LOPES DA ROCHA, «a lei da criminalidade informática», in Caderno de Ciencia de legislação, nº 8, 1993 pág. 66).

[8] Noçao abreviada de de *Interconnected networks*.

[9] Ver sore estes conceitos RITA COELHO SANTOS, em Tratamento jurídico penal da Transferencia de fundos Monetários atravez da Manipulaçao Ilícita dos Sistemas informticos, in Boletim da Faculdade de Direito, Studia iluridica 83, Coimbra, Coimbra Editora, 2005, Pág. 18 e segs.

4. A Informática Como Meio Para a Prática de Crimes

As tecnologias da informação e comunicação podem ser utilizadas enquanto instrumentos (muitas vezes mais eficazes quer nos danos causados quer no encobrimento da identidade dos seus autores) para a prática de crimes usuais da realidade corpórea e cujo tipo legal está previsto sem considerar a utilização dos meios tecnológicos como um elemento integrador do crime.

Tomemos por exemplo, a generalidade dos crimes contra a honra (injúrias ou difamação) que podem muito bem ser praticados pela inclusão dessas expressões ou acusações em páginas em linha, redes sociais, *blogs* ou difundindo-as por correio electrónico. Neste caso, a única interferência que o uso de meio tecnológico tem sobre o tipo legal será o meio utilizado para divulgação da expressão injuriosa ou difamatória, e o facto de tal meio de comunicação poder causar mais ou menos "danos" no bem jurídico ofendido.

Outro caso, será o facto de as tecnologias da informação e comunicação poderem ser utilizadas para cópia ilegal de obras protegidas por direitos de autor, face a facilidade com que se reproduzem *ficheiros áudio, vídeo, imagem, etc.*, em ambiente digital. Mais uma vez, o tipo legal permanece inalterado face à realidade corpórea ou incorpórea da cópia ilegal realizada.

Nestes casos, a informática não surge como elemento tipificador (ou sequer necessário) do crime, apenas como um instrumento utilizado para a sua prática, se bem que em determinados casos seja um instrumento potenciador da sua prática e/ou agravante dos danos deles decorrentes. Isto na medida em que a utilização dos meios associados ás tecnologias da informação e comunicação podem aumentar exponencialmente os danos decorrentes da lesão pela sua maior difusão através da internet (essencialmente nos crimes contra honra).

Embora admitimos que, como fenómeno social, a chamada "criminalidade informática" abarque esta realidade, na perspectiva substantiva estes crimes não têm merecido uma revisão face as novas formas digitais de os praticar. No entanto, nalguns casos o legislador sentiu a necessidade de criar novos tipos legais direccionados à sociedade de informação que vêm penalizar directamente actos que potenciam a violação dos mesmos bens protegidos. Por outro lado, já na perspectiva da obtenção da prova da

prática destes crimes, se tem pensado em novos dispositivos processuais capazes de uma mais eficaz recolha e conservação da prova digital. [10]

5. **A Criminalidade Informática**

Acompanhando a evolução tecnológica, o comportamento criminoso também evoluiu. Hoje praticamente toda a gente tem acesso a um computador, *smartphone* ou *tablet*, e a sua maior utilização consubstancia-se num maior risco para a sociedade, uma vez que, obviamente, se os meios informáticos facilitam tudo o resto na nossa vida, também facilitam a prática de crimes.

O prazer para o "criminoso digital" é grande pelo pouco risco que acarreta, pela possibilidade de praticar uma acção a grande distância e pela comodidade de na sua secretaria, ligado em rede, poder colher grandes frutos em pouco tempo e ao abrigo da grande dificuldade de detenção e investigação destes tipos de crimes, que por não terem fronteiras exigem uma intensa, e nem sempre fácil, cooperação internacional.

Nessa medida, cada vez mais esta é utilizada para lhe dificultar a vida, colocando novos problemas, criando novos tipos de agentes criminosos, diferentes dos tradicionais, e com modos operand muito próprios. No âmbito informático esta necessidade faz-se sentir ainda mais na medida em que há uma ameaça sobre sectores chave como a energia, transporte, telecomunicações, hospitais (etc.) áreas que hoje estão extremamente dependentes da informática.

Surgiu então fruto desta evolução tecnológica, um novo tipo de criminalidade, ligada de alguma forma à informática e aos computadores, a que se pode chamar criminalidade informática, que, em termos gerais pode definir-se como aquela que se traduz em condutas danosas para sociedade, concretizadas na utilização de um computador ou sistema de tratamento de dados, que funciona como objecto e/ou instrumento de acção, e que atenta contra bens jurídicos-penais, como a esfera privada do indivíduo ou seu património, através do acesso, recolha, armazenamento, introdução, alteração, destruição, intercepção ou transmissão informática (ou telemática) de dados.

---

[10] Cfr. CASTANHEIRA Rita; ANDRADE M. da Costa, Direito penal hoje: novos desafios e novas respostas, Coimbra: Coimbra Editora, 2009.

Estes tipos de crimes surgiram a partir da década de 60, e deu origem, desde aí, a vários casos mediáticos, principalmente nos Estados Unidos da América.

É necessário, no entanto delimitar o conceito de criminalidade informática, pois, dada a propensão para a informática se imiscuir na nossa ida, este conceito pode ser demasiado abrangente, abarcando um enorme número de condutas.

Não pode ser relevante para efeitos da criminalidade informática o facto de se furtar uma disquete ou cometer um crime de injúrias através do *email* ou de se utilizar o computador para efectuar planos para um homicídio cometido de forma "clássica". Para poderem ser caracterizados como fazendo parte da chamada criminalidade informática, parece-nos que os comportamentos delituosos deverão não apenas ter a intervenção de um computador, mas, além disso, revelar uma qualquer especificidade juridicamente relevante relativamente aos crimes em geral que resulte do uso da informática. Assim, a criminalidade informática será aquela que, além de ter como objecto ou instrumento um meio informático, revele, pelo uso desse meio, uma especial característica ou um qualquer elemento especial relevante para o cometimento daquele crime.

No entanto, poderão integrar a esta categoria, crimes cujo uso da informática, por exemplo, aumento exponencialmente à perigosidade para bens jurídicos, dificulte a detenção do seu cometimento e do seu agente, ou agrave de modo muito significativo as suas consequências. Pense-se por exemplo na difamação pela globosfera, ou no *hakers* que, com a propagação de um vírus inutiliza milhões de computadores com enormes prejuízos nas empresas. São crimes que ofendem interesses "clássicos", como o património ou a honra, mas que se servem da informática, e esse facto justifica a especial atenção do direito penal. Neste caso, o computador, *smartphone, tablets*... será o instrumento da prática dos crimes.

Por outro lado, abrange igualmente os crimes que ofendem bens directamente ligados ao meio informático, como o acesso ilegítimo ou o dano a programas informáticos, que visam proteger o próprio uso da informática e os seus aspectos característicos, como o *software* ou a navegação na *internet*. Aqui os computadores e a informática são o "próprio" objecto e também o instrumento do crime[11].

[11] Para mais detalhes vide CASTANHEIRA Rita; ANDRADE M. da Costa, Direito penal hoje: novos desafios e novas respostas, Coimbra: Coimbra Editora, 2009.

6. Tipologia e Modos de Execução

Os crimes relacionados a informática podem dividir-se em diferentes categorias.[12]

Desde logo podem identificar-se *crimes que recorrem à* meios *informáticos* , e que só podem ser cometidos com recurso ao meio informático, mas que dogmaticamente não se distinguem dos crimes tradicionais.[13]

Podem identificar-se depois crimes que podem definir como os crimes informáticos propriamente dito, aqueles cujo objecto e instrumento de execução é a informática, são praticados através da informática e contra elementos informáticos. Há ainda quem autonomize neste âmbito os crimes relativos a protecção de dados pessoais, devido a grande influência que os computadores exercem na pratica dos mesmos.

Na verdade os sistemas informáticos, de programação e tratamento de dados, actuam a distância e sem necessidade de contacto físico directo para poderem influenciar outros sistemas, e por isso mesmo oferecem uma vasta cobertura a este tipo de criminalidade, uma vez que basta uma ligação a um terminal, que por sua vez esteja ligado a uma rede para se poder cometer um crime pela informática, cuja execução, a pesar de muito variada, se resume a três grandes categorias: a manipulação, a espionagem, e a sabotagem.

Nesta medida, o seu modo de execução é a maior parte das vezes resultante de uma manipulação informática. Esta manipulação pode ser *input* ou *output*, conforme ocorra, respectivamente, na fase de integração de novos dados e tratamento destes ou na fase da saída de dados, dentro desta última categoria encontram-se por exemplo as falsificações de dados ou manipulação de ficheiro. Esta manipulação acaba por acontecer praticamente em todos os crimes informáticos, ainda que tenha menor peso do que eventualmente as outras formas utilizadas.

Quanto as manipulações anteriores e posteriores ao *input* ou *output*, como por exemplo a falsificação de documentos que irão servir posteriormente para formar uma

[12] Seguindo a divisão proposta por Rita Coelho Santos, ob. Cit., pág. 32 e segs., haveria crimes tipicamente informáticos , crimes essencialmente informáticos, e crimes acidentalmente informáticos.
[13] Nomeadamente a Burla informática e a devassa por meio de informática.

base de dados ou de documentos já imprimidos, apesar de frequentes, parecem já não revelar uma forma de crime informático, uma vez que a manipulação acontece antes ou depois do tratamento informático, dos dados perdendo assim a conexão com esse tratamento.

Outra das formas típicas de execução destes crimes é a espionagem informática, ou seja, a utilização ou acesso indevido de dados armazenados e por isso não acessíveis. Daí que também se designe esta forma de execução por " furto de dados "pois consiste precisamente em tomar conhecimento de informações ou dados ilegitimamente e contra a vontade e conhecimento do seu titular.

Além da manipulação, que consiste na alteração de dados, e da espionagem, que se taduz no conhecimento indevido dos mesmos, outra forma típica de cometimento destes crimes consiste na sabotagem informática, cujo objectivo é de qualquer modo afectar a integridade (corromper ou destruir) de dados ou sistemas informáticos, nesta forma não se aproveita os dados a que se acede em si, apenas se procura interferir no funcionamento dos mesmos e com isso obter algo.[14]

7. A Neo-Criminalização

A grande dificuldade da construção dos tipos relativos aos crimes informáticos prende-se com a intangibilidade dos bens, e com as novas formas de agressão aos mesmos, já referidas, e que dificultam sobremaneira a definição dos contornos destes tipos de crimes, justificando precisamente a criação de crimes informáticos específicos relativamente aos comuns.

Na verdade, há uma grande dificuldade na aplicação dos conceitos penais clássicos, que se tornam inadequados e obsoletos devido ao princípio da legalidade e a proibição da analogia *in malem partem, e* podem levar a insuperáveis lacunas de punibilidade, principalmente nos crimes de execução vinculada.

A interacção de processos entre os utentes e o computador levanta ainda problemas ao nível da acção e da chamada dimensão física do automatismo onde o carácter automático ou não automático dos dados, danificar ou tornar não utilizável coisa

[14] *Ibdem.*

alheia. O legislador quis apenas proteger especialmente os danos causados aos dados e programas informáticos.[15]

8. Dos Crimes Informáticos no Novo Código Penal Angolano

Mais de 40 anos passados sobre a data da Independência, os bens jurídicos tutelados pelo Código de 1886 não coincidem integralmente, como se calcula, com os interesses que a comunidade de cidadãos angolanos deseja ver hoje penalmente protegidos.

Tal como é defendido por TEREZA BELEZA, em comentário ao Anteprojecto do Código Penal cabo-verdiano, «O Código Penal de um país há-de, por força, reflectir os valores fundamentais da sociedade que o vai aplicar» [16].

Já nada justifica que Angola continue a definir e a tutelar valores fundamentais que prescindam à afirmação e ao progresso da sociedade angolana e ao livre desenvolvimento da personalidade do homem angolano, utilizando um instrumento legal completamente desajustado do ponto de vista da política e ciência moderna do direito penal. Em muitos aspectos, sobretudo no que se refere à sua parte especial, podemos, sem receio, considerar como arcaico, complexo, insuficiente e sem adequada correspondência com os valores de uma sociedade moderna e os interesses fundamentais do Estado angolano.

Com efeito, após longos anos dedicados à reforma penal em Angola, só em 2019 foi aprovado pelo parlamento angolano e em Novembro de 2020 publicado no diário da República, um verdadeiro Código Penal angolano.

9. Acesso Ilegítimo a Sistema de Informação Art. 438º

O acesso ilegitimo é o primeiro crime previsto no título VIII do futuro Código penal angolano. Neste tipo de crime, pune-se o mero acto de aceder, mesmo que não haja danos concretos, concretizando assim um crime de perigo abstracto, visando a protecção

---

[15] Cfr. CASTANHEIRA Rita; ANDRADE M. da Costa, Direito penal hoje: novos desafios e novas respostas, Coimbra: Coimbra Editora, 2009, pág. 232.
[16] Publicado in "Reformas Penais em Cabo Verde", da autoria do Dr. Jorge Fonseca.

antecipada e indirecta contra riscos de danos e de espionagem, criando obstáculo a danos que poderiam ocorrer se houvesse o acesso.

No entanto, apesar dessa protecção antecipada, também neste crime tem de se verificar o elemento subjectivo, a intenção de obter vantagem ilegítima para si ou para outrem[17]. Só é punido o acesso a sistema alheio se for feito com essa intenção.

Este crime como, o próximo, têm a sua base na "ilegitimidade" do acesso ou intercepção) constante da epígrafe de ambos e que se consubstanciam na falta de autorização. O acto em si materialmente não é ilícito, só o é na medida em que não haja uma autorização.

O tipo prevê uma agravação no caso de o acesso ser conseguido através de violação de regras de segurança[18], e se através desse acesso, o agente tomar conhecimento de segredo ou dados confidenciais, ou se a vantagem obtida for de valor consideravelmente elevado.

9.1. O Bem Jurídico

Este crime pune um dos mais característicos crimes informáticos, a chamada espionagem informática, ou "furto de informação", visando proteger o "domicílio informático", ou a segurança e privacidade de um sistema informático, que mais não é do que uma decorrência do próprio direito à privacidade, o bem jurídico.

No âmbito deste crime importa tecer considerações acerca daquele que é o ***ex libris*** dos crimes informáticos – o *Hacking* [19]

Na verdade este crime pune sem sombra de dúvida os acessos feitos com intenção lucrativas, mas este tipo de motivações está mais associado aos *Hackers*, agentes que efectivamente acedem ilegitimamente a sistemas mas com uma intenção clara e definida de com isso conseguirem benefícios materiais para si ou parar terceiros.

---

[17] Já não se prevê como elemnto intencional também a intenção de causar prejuízo pois geralmente quando se acede a um sistema informático o objectivo é obter uma vantagem. Ccaso seja outra a intenção já estaremos perante um crime de sabotagem informática.

[18] Como é o caso por exemplo da obtenção ilegítima de uma passworde de accesso.

[19] Na verdade, quando se fala em crimes informáticos a primeira coisa que surge na nossa mente é a figura do hacker, que é geralmente conhecido como todo o que comete um crime pela informática, o que não é necessariamente correcto.

Coisa diferente são os *Hackers* propriamente ditos (ou "quebra sistemas"), indivíduos com algum conhecimento técnico, nem sempre muito profundo e que se movem não pela possibilidade de uma vantagem patrimonial mas pelo mero *animus jocandi*, pelo mero desafio, curiosidade, aventura ou emoção de tentar quebrar as barreiras, geralmente sem nenhuma intenção criminosa inerente.

10. Intercepção Ilegítima em sistema de informação Art. 439º

O crime de intercepção ilegítima[20] e vulgarmente conhecido por "espionagem informática", é um tipo que pune os actos de escutar e vigiar sistemas de transmissão de dados à distância, e interceptar dados em curso de transmissão electronicamente a partir de terminais geralmente para obter *password*[21].

No fundo pune a "escuta" ilícita, como nos outros meios de comunicação[22]. O seu maior potencial de aplicação prático é nas comunicações pela *internet* (*chats emails*…).

Este crime tem também muitas conexões com o anterior, ambos se baseiam na ilegitimidade (falta de autorização) e inserem-se no mais amplo modo de execução da espionagem informática. A diferença é mais uma vez, o elemento subjectivo, pois o acesso ilegítimo exige o *animus lucrandi* enquanto este não exige qualquer intenção especifica.

10.1. O Bem Jurídico

Refere-se muitas vezes que o interesse protegido com esta incriminação é a exclusividade de comunicação de dados, no entanto, essa exclusividade está abrangida por um bem jurídico mais amplo, que é o da própria privacidade, ou o direito à vida privada. Deste modo, a incriminação prevê a punição da obtenção da informação através

[20] Quem, sem para tanto estar autorizado e através de meios técnicos, interceptar comunicações que se processam no interior de um sistema ou rede informática, a eles destinados ou deles provenientes.
[21] O chamado "Sniffing".
[22] Na verdade pune-se a intercepção ilícita, que é o " acto destinado a captar informaçoes cometidas num sistema autorizado de dados, através de dispositivos electromagnéticos, acusticos, mecânicos, ou outros.

da intromissão numa área de reserva. Também aqui não há nada de novo a nível dogmático, apenas o meio que é utilizado (a informática).[23]

11. Crime de Dano em Dados Informáticos Art. 440º

O crime de dano informático é um tipo que até agora a ordem jurídica angolana desconhece. Mas os "bens" corporizados em suportes informáticos são igualmente coisas que, como todas as outras, merecem e exigem, hoje em dia, tutela penal.

Este crime é de execução não vinculada, pois visa um resultado sem um processo causal tipificado, o que significa que estes conceitos devem ser preenchidos e cada caso, à semelhança do dano "clássico".

O legislador consagrou uma cláusula geral, pois é punido o agente que danificar os dados ou, por qualquer outra forma lhes afectar a capacidade de uso. É necessário ter atenção a esta norma pois parece-nos que tem de se exigir que a afectação da capacidade de uso seja relevante, e já não uma qualquer interferência por mínima que seja.

Em sentido prático inclui-se neste crime as condutas de espalhar "*vírus*"[24], "*Defacing*[25]", ou as chamadas "*bombas lógicas*[26]", quando por trás destes comportamentos esteja o intuito de causar prejuízo ou ter algum ganho.

Assim, este crime tem outras particularidades em relação ao crime de dano previsto no Código penal vigente, desde logo porque exige um elemento subjectivo típico, a intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo para si ou para terceiros. Configura assim, ao que nos parece, um crime de resultado cortado, na medida em que esse resultado não é parte integrante do tipo, apenas motivação do agente.

---

[23] *Cfr*. CASTANHEIRA Rita; ANDRADE M. da Costa, Direito penal hoje: novos desafios e novas respostas, Coimbra: Coimbra Editora, 2009.

[24] Esta forma globalmente conhecida de ataque ao meio informático consiste num conjunto de instruções que se podem reproduzir rapidamente e levam à inutilização de ficheiros e programas com uma grande capacidade de difusão. Cfr. João Carlos Cruz MACEDO «Direito Penal Hoje: Novos Desafios», Coimbra, Almedina editora, 2009, pág. 240.

[25] Alteração ilícita de páginas da internet com o objectivo de transmitir ideias ou provocações, o que afecta a imagem de entidades públicas ou privadas. Cfr. CASTANHEIRA Rita; ANDRADE M. da Costa, *Direito penal hoje: novos desafios e novas respostas*, Coimbra: Coimbra Editora, 2009, pág. 240.

[26] "Bomba lógica" ou "programa *crash*" são instruções clandestinas num programa autónomo que num determinado momento pré-definido actuam sobre os programas informáticos. Cfr. João Carlos Cruz MACEDO, «Direito Penal Hoje: Novos Desafios», pág. 240.

Na sua formulação teve-se em consideração, a Convenção Sobre o *Ciber crime* subscrita pelos Estados-Membros do Conselho da Europa (e não só) o Código Penal alemão e a lei da criminalidade informática portuguesa[27].

11.1. O Bem Jurídico

Parece-nos que o bem jurídico em causa neste crime é semelhante à propriedade, protegida no crime de dano previsto no C.P vigente.

O dano protege a propriedade contra lesões que atinjam directamente a existência ou o estado da coisa, ou seja, protege o direito do proprietário de fazer da coisa o que quiser, retirando dela as utilidade que pode oferecer.

Ora, os programas ou dados informáticos, apesar de não terem uma materialidade semelhante às coisas que existem autónomas do seu suporte, não deixam de ser "coisas" protegidas. São coisas imateriais, mas que são apreensíveis empíricamente, estão expostas à acção do homem e são susceptíveis de sobre elas ser exercido direito de propriedade e de serem destruídas e danificadas pelos mais diversos meios (*vírus, hackers…*) nessa medida podem ser objecto do crime de dano.

Na verdade, a especificidade deste crime reside no facto de não se atacar a substância de um objecto, mas as informações contidas em determinado dado ou programa, no entanto as formas de agressão são semelhantes, uma vez que também aqui é punido o acto de destruir, danificar ou tornar não utilizável coisa alheia. O legislador quis apenas proteger especialmente os danos causados aos dados e programas informáticos.[28]

12. Sabotagem Informática Art. 441º

Este é um crime de dano, verdadeiramente é mais um crime de dano informático do que o próprio crime de dano em dados e programas informáticos, uma vez que não se exige aqui o *animus lucrandi* nem se faz referência ao elemento da autorização [29]. A diferença entre os dois crimes é a intenção subjacente à conduta, pois, neste exige-se

---

[27] Para mais detalhes vide Vasco Gandão RAMOS, Relatório do Anteprojecto do Código Penal Angolano, 2016, pág. 110.

[28] Cfr. CASTANHEIRA Rita; ANDRADE M. da Costa, Direito penal hoje: novos desafios e novas respostas, Coimbra: Coimbra Editora, 2009, pág. 242.

[29] Neste sentido, FARIA COSTA, «Algumas reflexões…..» Cit. Pág. 111.

intenção de entravar o funcionamento dos referidos sistemas, ou seja, este é também um crime intencional, mas a intenção é apenas entravar o funcionamento do sistema e já não qualquer benefício para o agente. Este elemento subjectivo visa combater as condutas que têm como objectivo puro e simples o ataque aos sistemas informáticos[30], pois se esse ataque tiver alguma intenção lucrativa, ou de prejudicar o utente, já estaremos no âmbito do crime anterior.

Não deixa de ser curioso que a lei pune mais gravemente a intenção de atacar os sistemas informáticos do que a intenção de atacar os seus proprietários ou utentes através deles. Parece que essa lei hiperboliza um pouco a violação desses sistemas, e está um pouco desequilibrada nas suas sanções.

Este é um crime de execução livre, os meios empregados são quaisquer que sejam idóneos a produzir um resultado, utiliza-se a técnica dos exemplos padrão, ou seja, além dos meios expressamente previstos, qualquer outra forma de ingerência preenche o tipo, o que desde logo o aproxima do crime anterior quanto à conduta[31]

Neste crime enquadra-se as condutas de dano puro e simples em sistemas informáticos, ou seja, sem qualquer intenção que não seja a de os afectar. Assim, aplica-se, tal como o crime anterior e até em maior medida a propagação de "víros e vermes", quando a causa seja apenas estragar ou encravar os computadores ou até ao chamado "*mail bombing*" ou "*spam*", conduta que nos parece também enquadrável na clausula geral deste crime.

Como vimos, este crime tem muitos pontos contíguos com o anterior, pois as condutas punidas são extremamente semelhantes, a única diferença parece ser mesmo a intenção por trás do dano, sendo que o legislador pune mais gravemente o dano com a intenção de encravar os sistemas.

---

[30] Como por exemplo os ataques dos (Denial Service), que consistem num ataque às estruturas técnicas de um sistema informático. Por isso se considera que é um crime contra o sistema informático. No entanto não parece que só por se exigir aquela intenção se projecta o sistema em si e não a sua utilidade para os seus proprietários e usuários.

[31] Na verdade no dano, está em causa qualquer conduta que afecte a capaidade de uso dos dados ou programas informáticos, enquanto na sabotagem está em causa qualquer forma de interferir em sistemas informáticos . Esta distinção parece quase não existir, e a diferença terá que se retirar da intenção subjacente à conduta.

12.1. O Bem Jurídico

No seguimento do exposto, parece-nos que o bem jurídico protegido é semelhante ao anterior, o que está em causa é a protecção da propriedade do utente do sistema informático, ou seja, protege-se o interesse do proprietário ou do utente de um sistema informático em que estes estejam a funcionar corretamente evitando os danos directos nos equipamentos informáticos e os danos consequenciais.

É recorrente dizer-se que está em causa a autonomia do valor acrescido que é a informática e a possibilidade que ela oferece de tratamento de dados, está em causa a máquina e o seu funcionamento extremamente importante e em certos sectores. Nessa medida, neste crime está em causa o sistema informático, enquanto no anterior estão em causa dados ou programas informáticos. O que não deixa de ser verdade, mas o sistema está sempre ao serviço do seu proprietário ou dos seus utentes, que dele retiram utilidade.[32]

13. Falsidade Informática Art. 442º

O crime de falsidade informática, está previsto no art. 442º, pelo que esta norma tem como objecto as falsificações efectuadas por um computador.

O tipo é preenchido com a exploração não autorizada de dados falsos apresentados como verdadeiro, fazendo um computador reagir a esses dados falsos como se tratassem de dados autênticos e abrange todas as falsificações como a introdução não autorizada de dados ou a posterior alteração dos mesmos.

No fundo o resultado é análogo ao da falsidade de um documento e este tipo é apenas uma decorrência do tipo clássico de falsificação (art.216º do C.P velhote), apenas jogando com as especificações necessárias para adaptá-lo ao específico meio informático. Em consonância com as concepções doutrinárias sobre esta matéria, a falsificação de documentos é, em primeiro lugar, a elaboração de documento inteiramente falso (contrafacção), mas é-o, também, a alteração de documento verdadeiro, a utilização abusiva da assinatura de outra pessoa aposta no respectivo suporte documental para elaborar documento falso e, ainda, a falsidade intelectual. [33]

---

[32] Cfr. CASTANHEIRA Rita; ANDRADE M. da Costa, Direito penal hoje: novos desafios e novas respostas, Coimbra: Coimbra Editora, 2009. 243 – 245.

[33] Cfr. RAMOS Vasco Grandão, Relatório do Anteprojecto do Código Penal Angolano,2016, pág. 74.

Daí a referência que faz o tipo: *de tal modo que a visualização produza os mesmos efeitos de um documento falso.*

13.1. O Bem Jurídico

É perceptível, então, que não se protege qualquer bem jurídico novo, nem sequer algum bem jurídico especificamente informático, o bem protegido é a segurança e fiabilidade de documentos e a protecção contra o engano nas relações jurídicas, ou a veracidade na reconstituição das relações jurídicas, de forma exactamente igual aos interesses protegidos pelo direito penal clássico relativamente às outras falsidades. A única especificidade deste tipo consiste no *modus operandi* onde releva a execução pelo meio informático.[34]

No artigo 442º do novo Código Penal angolano prevê-se o crime de "falsidade informática". O agravamento da punição deste tipo (visto que o bem jurídico é efectivamente o mesmo com o de falsidade de documentos) explica-se pela sua gravidade acrescida, uma vez que se trata de tipo de crime de execução fácil para quem domine os meios de o praticar, mas difícil de prevenir, detectar e combater. Este facto, somado às especificidades e até complexidades da forma de incorporação das declarações e correspondentes dados no respectivo suporte justificam, a nosso ver, a tipificação autónoma do crime de falsidade informática.[35]

14. Crime de Burla Informática Art. 443º

À primeira vista percebe-se que este tipo de crime pouco tem a ver com a "burla clássica" na medida em que não há aqui aquele elemento característicos de introduzir outra pessoa em erro, fazendo que essa pessoa, por esse motivo, pratique determinados actos que a prejudiquem. Na verdade, a burla exige uma "muito particular forma de comportamento" que se traduz num meio enganoso seja a causa efectiva do erro em que se encontrava a vítima, exigindo-se o chamado duplo nexo de imputação objectiva.

---

[34] CASTANHEIRA Rita; ANDRADE M. da Costa, Direito penal hoje: novos desafios e novas respostas, Coimbra: Coimbra Editora, 2009, pág. 238.
[35] Cfr. RAMOS Vasco Grandão, Relatório do Anteprojecto do Código Penal Angolano, 2016, pág. 75.

Na burla informática não existe essa exigência de um meio ardiloso, nem tão pouco é uma exigência do tipo que a vítima tenha uma parte activa no processo de execução do crime. Exige-se apenas a intenção de causar um prejuízo patrimonial, e para esse efeito utilizando um meio informático, ou mais precisamente, interferindo num meio de tratamento de dados.

A incriminação da burla informática[36] tem como escopo sobretudo proteger a fiabilidade das transferências electrónicas de fundos, especialmente o abuso dos levantamentos nas máquinas automáticas. A jurisprudência tende a considerar neste tipo de crimes os casos de aproveitamento de cartões de crédito alheios.

14.1. O Bem Jurídico

O bem jurídico aqui é o património, o tipo visa proteger a esfera patrimonial, em termos semelhantes ao crime da burla clássica. Não há, assim também neste crime nenhum bem jurídico diferente, noutros termos não há a proteção de um bem jurídico especificamente informático.[37]

15. Reprodução Ilegítima de Programas Protegidos Art. 444º

Os programas informáticos são um dos principais alvos da criminalidade informática, uma vez que são muito caros, fruto de grandes investimentos e facilmente copiados, visam proteger o *softwere* ou o *logiciel*, prevendo o crime de reprodução ilegítima de programas protegidos. Este tipo consagra uma grande evolução relativamente à protecção os programas informáticos.

---

[36] Art. 407º do futuro código penal: Que, com propósito de obter para sí ou para terceiro vantagem patrimonial ilícita:

a) Interferir no resultado de tratamento de dados mediante estruturação incorrecta de programa informático, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização, ou mediante intervenção, por qualquer outro modo não autorizado, no processamento;
b) Usar programas, dispositivos electrónicos ou outros meios que, separada ou conjuntamente, se destinem a diminuir, alterar ou impedir, no todo ou em parte, o normal funcionamento ou exploração do serviço de telecomunicações e, pelas formas descritas, causar a outrem prejuízos de natureza patrimonial é punido com as penas do artigo 405º do futuro código penal.

[37] Para mais detalhes ver ANDRADE da Costa Manuel et. Neves Rita Castanheira, «Direito Penal Hoje: Novos Desafios», Coimbra, Almedina editora, 2009.

Este tipo abrange a chamada pirataria informática, e é de todos o mais comum entre nós.

Geralmente assume duas formas, ou a venda em locais públicos ou a instalação em locais privados, como escritórios ou empresas.

Na verdade, hoje em dia praticamente todos cometem ou pelo menos fecham os olhos, a este tipo de pirataria. Quem não tem instalado num computador um anti-virus recente ou a nova versão de algum programa de reproduzir música ou processar texto? E haverá a respectiva licença? Hoje em dia este crime de ameaça tornar-se num verdadeiro flagelo, uma vez que já não é utilizada a reprodução ilegítima apenas porque é mais barato, mas simplesmente porque é grátis, devido à crescente utilização de programas, em que se partilha informação livre e gratuitamente entre os utilizadores on-line.

Neste crime englobam-se as condutas de reproduzir, divulgar ou comunicar ao público um programa informático protegido por lei.

Esta norma é uma " norma penal em branco", utiliza técnica do reenvio externo, pois remete para outra legislação para concretizar o que é um programa protegido por lei.

Este crime afasta-se dos modos de execução dos outros (manipulação, sabotagem e espionagem) uma vez que não visa interferir nos dados, mas simplesmente reproduzi-los.

As condutas de divulgar ou comunicar ao público não levantam questões de maior, no entanto é necessário determinar o sentido de reproduzir.

Parece-nos que a reprodução implica não só a cópia de vários exemplares, mas também a fixação na memória do computador. De fato já se está a reproduzir o programa podendo inclusivamente instala-lo e passa-lo a outros pela internet, correndo-o livremente através dos programas, e desse modo haveria uma grande lacuna de punibilidade se a fixação na memória do computador não fosse considerada uma reprodução para os efeitos deste tipo.

Também parece claro que, quem apenas utiliza o programa não pode ser punido, pois não preenche nenhum dos elementos do tipo objectivo[38].

[38] A questão coloca-se na medida em que é difícil muitas vezes saber quem fez a reprodução.

A lei terá de ser aperfeiçoada, mas parece-nos seguindo Lopes Rocha, que hoje em dia não se poderá exigir a cumulação dos requisitos, quer porque a lei já dá a devida cobertura às cópias legítimas para o uso privado, quer porque a evolução e estado da comunicação e partilha on-line, já referida anteriormente, poderia abrir lacunas de punibilidade.

15.1. O Bem Jurídico

Tem se vindo a considerar que o bem jurídico protegido é o programa, e dessa forma vislumbrar-se-á aqui o único bem jurídico verdadeiramente novo na doutrina.

No entanto, parece-nos que a pesar de com esta norma se proteger os programas informáticos, estes são apenas objectivos da acção, o bem jurídico em causa é a propriedade intelectual sobre os mesmos. De facto, os programas em si, ou a sua integridade estão protegidos nas normas já analisadas, nomeadamente no crime de dano relativo a programas informáticos e na sabotagem informática. Aqui o que está em causa é a reprodução ou divulgação procurando-se defender as patentes, evitando cópias desses mesmos programas, pelo que nos parece, o bem jurídico em causa é a propriedade intelectual sobre a criação desses programas.

Dessa forma, também aqui não haveria um bem jurídico específico informático, mas apenas a protecção de uma forma de violação do bem referido (como se protege as patentes sobre obras ou patentes industriais), pois, como é reconhecido, a informática é um veículo fácil e privilegiado de copiar *softwere*.

Conclusão

Importa, agora dar conta dos resultados alcançados na nossa longa e difícil caminhada, sobre o estudo teorético, mas de grande relevo prático, que nos propomos no princípio do nosso percurso, os crimes informáticos no ordenamento jurídico angolano, concretamente o regime geral dos crimes de falsidade informática, o de dano de dados informáticos, o de burla informática dentre outros, conclusões:

É ponto assente de que os crimes informáticos podem definir-se em sentido amplo como aqueles em que os sistemas de tratamento automático de dados e de informação são

objectos ou instrumentos do crime, ou este está de forma significativa ligado à utilização desses sistemas, e que a sua evolução normativa ao nível da criminalidade informática começou no início dos anos 70 visando essencialmente a protecção da vida privada para fazer face às novas possibilidades de recolha, transmissão e armazenamento de dados possibilitada pela informática.

Relativamente aos tipos de crimes informáticos, é de salientar que no que respeita ao bem jurídico protegido nos crimes informáticos, é ponto assente de, que não se protege qualquer bem jurídico novo, nem sequer algum bem jurídico especificamente informático, e que tal, como por exemplo, nos crimes de falsidade de documentos tradicional, o bem protegido é a segurança e fiabilidade de documentos e a protecção contra o engano nas relações jurídicas, ou a veracidade na reconstituição das relações jurídicas de forma exactamente igual aos interesses protegidos pelo direito penal clássico relativamente às outras falsidades. A única especificidade deste tipo consiste no *modus operandi* onde releva a execução pelo meio informático.

Neste sentido e do mesmo modo, sucede com o crime de Burla Informática, onde o bem jurídico protegido é o património, no crime de dano informático protege-se a propriedade etc.

Já no que diz respeito aos outros crimes informáticos como por exemplo no crime de acesso ilegítimo, onde pune-se o mero acto de aceder, mesmo que não haja danos concretos, concretizando assim um crime de perigo abstracto, visando a protecção antecipada e indirecta contra riscos de danos e de espionagem, criando obstáculo a danos que poderiam ocorrer se houvesse o acesso. E no que diz respeito ao bem jurídico protegido neste crime, o "domicilio informático", ou a segurança e privacidade de um sistema informático, que mais não é do que uma decorrência do próprio direito à privacidade o bem jurídico.

Por outro lado, falou-se também do crime de Reprodução Ilegítima de programa protegido, e este tipo abrange a chamada pirataria informática, e é de todos o mais comum entre nós, onde englobam-se as condutas de reproduzir, divulgar ou comunicar ao público um programa informático protegido por lei. E considera-se que o bem jurídico em causa é a propriedade intelectual sobre os mesmos.

Huambo, 12 de Novembro de 2020

Jelssimi Moisés da Cunha

Referências bibliográficas

DIAS J. F.A.Et al, *Comentários Conimbricense do código penal*, 2ª Ed. Coimbra: Coimbra Editora, 2012.

ANDRADE, Manuel da Costa, In Comentário Conimbrincense do Código Penal, Parte Especial Tomo I, Coimbra, 1999.

CASTANHEIRA Rita; ANDRADE M. da Costa, *Direito Penal Hoje: novos desafios e novas respostas*, Coimbra: Coimbra Editora, 2009.

VENÂNCIO Pedro Dias, *Lei do Cibercrime*, Coimbra: Coimbra Editora.

BBARBAS, STELA, MARCOS DE ALMEIDA NEVES, "*Direito ao Patrimonio Genético*", Almedina, 1998.

COSTA JOSÉ DE FARIA, " *A linha" (Algumas reflexões sobre responsabilidade em um tempo de "técnica" e de bio-ética), Linhas de Direto Penal e de Filosofia*. Coimbra: Coimbra Editora.

RAMOS V. Grandão, *Relatório do Anteprojecto do Código Penal Angolano*, Luanda, 2016.

MACEDO João Carlos Cruz Barbosa, in "*Direito Penal Hoje: Novos desafios e novas respostas*, Coimbra, Almedina editora, 2009.

Legislações

Constituição da República de Angola

Código Penal Angolano

Novo Código Penal Angolano