Região Administrativa Especial de Macau

Regime Jurídico da Intercepção e Protecção de Comunicações

Documento de Consulta

Período de Consulta: 26 de Setembro a 09 de Novembro de 2018

Polícia Judiciária

2018

Índice

Introdução 3

1. Protecção dos direitos fundamentais e seu aperfeiçoamento 5

2. Ajustamento das disposições vigentes 6

2.1 Tipos de crimes aplicáveis 6

2.2 Tipos de comunicações que podem ser alvo de intercepção 8

2.3 Meios de intercepção 8

2.4 Prazo de duração da intercepção de comunicações 9

2.5 Definição do prazo do procedimento 9

2.5.1 Prazo para entrega dos elementos recolhidos durante a intercepção de comunicações 9

2.5.2 Data de início para o exame dos autos 9

3. Conteúdo novo 10

3.1 Consulta e extracção do conteúdo de comunicações armazenado por ordem do juiz 10

3.2 Estabelecimento dos deveres para os operadores de telecomunicações e os prestadores de serviços de comunicações em rede 11

3.2.1 Dever de colaboração 11

3.2.2 Dever de conservação 12

3.3 Penalização de outros actos irregulares 12

4. Aplicação subsidiária das disposições do Código de Processo Penal 13

5. Data da entrada em vigor 13

Extractos das respectivas legislações de outros países e regiões 14

Tabela para apresentação de opiniões e sugestões relativas à legislação 22

Introdução

As escutas telefónicas são um meio de obtenção de provas que desempenham um papel indispensável na investigação dos crimes com características organizadas, dissimuladas ou daqueles praticados com recurso ao telefone para as polícias de todo o mundo. Porém, como as escutas telefónicas envolvem os direitos fundamentais de liberdade e de sigilo dos meios de comunicação da população, a sua realização num Estado de Direito deve preencher as disposições relativas aos meios, formalidades e pressupostos legais, bem como deve estar sob um controlo judicial extremamente rigoroso.

As escutas telefónicas são já actualmente um dos meios legais de obtenção de prova em Macau e estão previstas nos artigos 172.° a 175.° do Capítulo IV do Código de Processo Penal. A sua forma concreta de aplicação consiste na intercepção ou gravação de conversações ou comunicações telefónicas, realizadas pelo órgão de polícia criminal, e **só podem ser ordenadas ou autorizadas por um juiz**, se se reunirem os requisitos legais para a obtenção de provas necessárias na investigação do crime. O regime é extensivamente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone.

O regime supracitado vigora há mais de 20 anos e o desenvolvimento e popularização das tecnologias de comunicações destes anos marcaram mudanças radicais nas formas de comunicação. As chamadas tradicionais de voz por telefone têm sido utilizadas cada vez menos, enquanto as chamadas de voz através da internet, bem como as formas de comunicação escrita, com som, símbolos, imagens ou vídeo, tornaram-se o fluxo principal, com incidência na nova realidade da actuação criminosa, pelo que a revisão do regime das escutas telefónicas se torna, de facto, urgente, necessária e racional.

Assim, foi efectuado um estudo aprofundado acerca dos conteúdos de textos semelhantes redigidos nos últimos anos, a nível de direito comparado, no qual, por um lado, se tomaram como referência os regimes jurídicos avançados de intercepção de comunicações de alguns países e regiões, nomeadamente Portugal, Alemanha, Japão, Região Administrativa Especial de Hong Kong e o território de Taiwan, por outro, foram adoptadas as sugestões dos serviços competentes e diferentes juristas, apresentadas em 2013 pelo Governo da RAEM, por ocasião da revisão do Código de Processo Penal, aludindo já à revisão do actual regime das escutas telefónicas na modalidade de lei avulsa e a validade da autorização da intercepção. Posteriormente, desenvolveu-se o trabalho de revisão do actual regime das escutas telefónicas.

Tendo em consideração as necessidades ao nível da execução da lei em Macau e do desenvolvimento da tecnologia das telecomunicações locais, elaborou-se uma estrutura fundamental do projecto, após troca de comunicações com os serviços relativos a assuntos da Justiça, de modo a preparar a lei avulsa do "Regime Jurídico da Intercepção e Protecção das Comunicações", que **foi apreciada pelo Conselho Executivo, tendo sido ouvidas as opiniões técnicas do Conselho Consultivo da Reforma Jurídica e do Gabinete para a Protecção de Dados Pessoais**. Nestes termos, procedeu-se à elaboração do presente documento de consulta sobre o "Regime Jurídico da Intercepção e Protecção de Comunicações", esperando que através do mesmo seja possível recolher e ouvir amplamente as opiniões e sugestões da população e dos diversos sectores da comunidade acerca da pretendida revisão, pretendendo-se ainda, por via deste projecto de legislação, consagrar um equilíbrio entre a investigação criminal, o combate ao crime e a protecção dos direitos dos cidadãos relativos às comunicações.

1. Período de consulta:
   26 de Setembro a 09 de Novembro de 2018.

2. Meios de apresentação:
   (1) Por carta: Enviar ou entregar directamente na Polícia Judiciária, sita na Avenida da Amizade, n.º 823, RAEM.

   (2) Por via electrónica: Entregar através do acesso ao portal do Governo da RAEM (http://www.gov.mo) ou à página electrónica específica no website da PJ (http://www.pj.gov.mo/pt/rjipc).

3. Para facilitar a organização, por favor, indique no envelope, na capa ou no cabeçalho da folha: "Sugestões e Opiniões sobre o Regime Jurídico da Intercepção e Protecção de Comunicações".

4. O documento de consulta estará disponível no endereço:
   Do portal do Governo da RAEM (http://www.gov.mo) ou da página electrónica específica no website da PJ (http://www.pj.gov.mo/pt/rjipc).

5. Declaração de confidencialidade:
   As pessoas que pretendam manter a confidencialidade das suas opiniões e sugestões devem indicá-lo expressamente no momento em que estas forem apresentadas ou seleccionar a coluna "Declaração de Confidencialidade" constante na "Tabela para apresentação de opiniões e sugestões relativas à legislação" anexada ao documento de consulta.

1. Protecção dos direitos fundamentais e seu aperfeiçoamento

Como referido na introdução, as escutas telefónicas envolvem os direitos fundamentais dos residentes no que diz respeito à liberdade e ao sigilo dos meios de comunicação. Nestes termos, durante a redacção do presente "Regime Jurídico da Intercepção e Protecção de Comunicações" tem-se atendido com muito rigor à protecção fundamental existente, ou seja, têm-se ponderado, conforme o artigo 32.° da Lei Básica da RAEM[1], os direitos fundamentais dos residentes no âmbito da liberdade e do sigilo dos meios de comunicação. Procede-se assim, com base nessa disposição, ao aperfeiçoamento do regime das escutas vigente, nomeadamente no seu contexto e mecanismo de protecção.

Em certo sentido, a elaboração do presente "Regime Jurídico da Intercepção e Protecção de Comunicações" não é a criação de um novo regime, mas apenas um aperfeiçoamento do regime de escutas telefónicas que se encontra regulado no Código de Processo Penal vigente. Significa que os domínios de protecção inerentes não irão ser prejudicados, pretendendo-se manter os princípios ou o teor fundamental do regime existente, nos seguintes termos:

(1) A intercepção de comunicações só pode ser efectuada mediante a **ordem ou autorização prévia do juiz**;

(2) A intercepção de comunicações só pode ser efectuada se houver razões para crer que a diligência se revelará de grande interesse para a descoberta da verdade ou para a prova quanto a crimes especificados;

(3) Nos termos da lei, todos os requisitos e condições são estabelecidos sob pena de nulidade, ou podem até constituir proibição de prova;

(4) É proibida a intercepção de conversações ou comunicações entre o arguido e o seu defensor, salvo se o juiz tiver fundadas razões para crer que elas constituem objecto ou elemento de crime;

(5) Da intercepção de comunicações é lavrado auto, do qual, junto com os respectivos dados adquiridos, é informado o juiz que tiver ordenado ou autorizado as operações;

(6) No caso de o juiz considerar os elementos recolhidos relevantes para a

[1]Nos termos do artigo 32.º da Lei Básica da RAEM, "Nenhuma autoridade pública ou indivíduo poderá violar a liberdade e o sigilo dos meios de comunicação dos residentes, sejam quais forem os motivos, excepto nos casos de inspecção dos meios de comunicação pelas autoridades competentes, de acordo com as disposições da lei, e por necessidade de segurança pública ou de investigação em processo criminal."

prova, ordena que se juntem ao processo; caso contrário, ordena a sua destruição. Todos os participantes nas operações ficam vinculados ao dever de segredo relativamente àquilo de que tenham tomado conhecimento;

(7) O arguido, o assistente bem como as pessoas sujeitas à intercepção de comunicações têm o direito de examinar o auto.

Com base no exposto, o "Regime Jurídico da Intercepção e Protecção de Comunicações" irá definir disposições processuais mais rigorosas e detalhadas, irá também sancionar os eventuais actos irregulares respeitantes à intercepção de comunicações, visando reforçar a protecção dos residentes contra violação dos seus direitos e liberdade no que concerne aos meios de comunicação.

Para as matérias que não foram integradas na protecção exclusiva do "Regime Jurídico da Intercepção e Protecção de Comunicações" recorre-se subsidiariamente às disposições do Código de Processo Penal, de forma a colmatar as eventuais lacunas na protecção jurídica.

2. Ajustamento das disposições vigentes

2.1 Tipos de crimes aplicáveis

O n.º 1 do artigo 172.º do Código de Processo Penal vigente estipula que a intercepção ou gravação de conversações ou comunicações telefónicas pode ser realizada quanto a crimes:

(1) Puníveis com pena de prisão de limite máximo superior a 3 anos;

(2) Relativos ao tráfico de estupefacientes;

(3) Relativos a armas proibidas, ou a engenhos ou matérias explosivos ou análogos;

(4) De contrabando;

(5) De injúrias, de ameaças, de coacção e de intromissão na vida privada, quando cometidos através de telefone.

Pode-se ver das disposições acima referidas, que o âmbito de aplicação do actual regime das escutas telefónicas incide principalmente sobre crimes graves e crimes cuja recolha de provas só possa ser realizada mediante as escutas telefónicas. Todavia, de acordo com a situação da criminalidade de Macau ou os desafios enfrentados no trabalho de investigação, observa-se:

(1) O crime organizado, os crimes relativos ao branqueamento de capitais, ao terrorismo, ao tráfico de pessoas, crimes contra a segurança nacional, e o crime informático, revelam um alto nível de gravidade e perigosidade, dissimulação, organização e destacam-se pela sua transterritorialidade. Para além disso, os actos e o *modus operandi* destes crimes são relativamente complexos e é difícil obter provas com a realização das diligências de investigação tradicionais;

(2) Embora a pena de prisão para o crime de violação de domicílio (artigo 184.º do Código Penal) seja de limite máximo de um ano, a forma prática do seu cometimento, com a previsão do n.º 2 do mesmo artigo, é por via telefónica para a habitação de outra pessoa, portanto, os órgãos de investigação quase não podem obter provas por outros meios para além das escutas telefónicas.

Por isso, propõe-se que os crimes supracitados sejam integrados no âmbito da aplicação da intercepção de comunicações.

Por outro lado, tendo em conta que, na actual legislação de Macau, não existe o crime de contrabando, deve este ser eliminado.

Em resumo, sugere-se, na elaboração da presente proposta de lei, um ajustamento para que a intercepção de comunicações seja aplicável aos crimes:

(1) Puníveis com pena de prisão de limite máximo superior a 3 anos;

(2) Relativos ao tráfico de estupefacientes;

(3) Relativos a armas proibidas, ou a engenhos ou matérias explosivos ou análogos;

(4) De injúrias, de ameaças, de coacção, de violação de domicílio, e de intromissão na vida privada, quando cometidos através de telecomunicações;

(5) Relativos à criminalidade organizada;

(6) Relativos ao branqueamento de capitais;

(7) Relativos ao terrorismo;

(8) Relativos ao tráfico de pessoas;

(9) Relativos à ameaça da segurança nacional;

(10) Informáticos.

2.2 Tipos de comunicações que podem ser alvo de intercepção

À medida que o modelo de comunicação se modifica, a lei relativamente à obtenção de provas deve adaptar-se à evolução dos tempos, pelo que se tomam como referência as legislações de outros países e regiões, nas quais foram criadas normas expressas quanto a intercepção de mensagens não sonoras, nomeadamente, símbolos, escritas, imagens ou outras mensagens.

Tendo em consideração a situação real de Macau, sugere-se que possam ser objecto de intercepção das comunicações todos os símbolos, escritas, imagens, sons, desenhos ou comunicação e troca de informações de qualquer natureza emitidos, transmitidos ou recebidos com recurso às telecomunicações[2].

A par disso, para que a nova lei seja aplicável a situações imprevisíveis no âmbito desta proposta de lei, propõe-se que seja feita uma análise da disposição prevista no artigo 175.º do Código de Processo Penal vigente para que se torne mais claro que o regime de intercepção de comunicações seja aplicável às comunicações transmitidas por qualquer meio técnico diferente das telecomunicações.

2.3 Meios de intercepção

O n.º 1 do artigo 172.º do Código de Processo Penal vigente estipula expressamente que há duas formas de escutas telefónicas: intercepção ou gravação de voz. Contudo, não se encontram previstos expressamente os meios de intercepção quanto às conversações ou comunicações transmitidas por qualquer meio técnico a que se refere o artigo 175.º do CPP.

Atendendo que é sugerido no presente documento de consulta a alteração dos tipos de comunicações admissíveis, torna-se necessário proceder a ajustamentos quanto aos meios de execução. Após a análise das demais disposições de outros países e regiões, nomeadamente da Região Administrativa Especial de Hong Kong e do território de Taiwan, os meios de intercepção de comunicações previstos expressamente para efeitos de investigação criminal tendem a ser cada vez mais diversificados.

Neste sentido, propõe-se que nos meios de intercepção de comunicações se incluam escuta, intercepção, gravação, transcrição, cópia de voz ou imagem, entre outros tipos de informações, bem como outros meios semelhantes que são

[2]Nos termos da alínea 1) do artigo 3.º da Lei n.º 14/2001 (Lei de Bases das Telecomunicações): "telecomunicações — a transmissão, emissão ou recepção de símbolos, sinais, escrita, imagens, sons ou informações de qualquer natureza, por fios, radioelectricidade, óptica ou outros sistemas electromagnéticos".

necessários, legais e úteis à investigação criminal.

2.4 Prazo de duração da intercepção de comunicações

Visto que as escutas telefónicas e a intercepção de comunicações envolvem o sigilo das comunicações dos residentes, torna-se necessário definir, por meio da lei, as limitações dos prazos de intercepção relativamente à sua execução. Tomando como referência as respectivas disposições legais de outros países e regiões, geralmente estão definidos o prazo relativo à intercepção de comunicações e as respectivas disposições de renovação.

Assim, propõe-se a estipulação de um prazo para a intercepção de comunicações, que deve ser efectuada por um período máximo de três meses, que pode ser renovado, mediante pedido submetido ao juiz, desde que os requisitos para a realização dessa intercepção continuem a existir, não podendo cada renovação exceder um período máximo de três meses.

2.5 Definição do prazo do procedimento

2.5.1 Prazo para entrega dos elementos recolhidos durante a intercepção de comunicações

O n.º 1 do artigo 173.º do Código de Processo Penal determina que, da intercepção ou gravação é lavrado um auto, pelo órgão de polícia criminal, o qual, juntamente com as fitas gravadas ou elementos análogos, é "imediatamente" levado ao conhecimento do juiz competente.

Dado que existem interpretações divergentes na compreensão da palavra "imediatamente", propõe-se que a expressão seja alterada para "até ao fim do prazo concedido pelo juiz", a fim de explicitar o prazo da entrega dos elementos recolhidos na intercepção de comunicações, para que o respectivo juiz possa proceder à fiscalização, selecção e decisão sobre os procedimentos subsequentes.

2.5.2 Data de início para o exame dos autos

No n.º 3 do artigo 173.º do Código de Processo Penal vigente, está previsto que o arguido e o assistente, bem como as pessoas cujas conversações tiverem sido escutadas, podem examinar os autos, mas a data de início para este efeito não se encontra fixada. Com o intuito de facilitar o exercício de tal direito por parte do arguido, assistente e pessoas sujeitas à intercepção de comunicações, sugere-se que seja definido que as pessoas em causa podem ter acesso aos autos a partir da data de notificação da acusação e obter, à sua custa, cópia dos elementos naqueles referidos. É de salientar que esta sugestão corresponde completamente às disposições gerais do

citado código relativas ao direito do arguido a examinar os elementos dos autos.

3. Conteúdo novo

3.1 Consulta e extracção do conteúdo de comunicações armazenado por ordem do juiz

Em relação à investigação e à recolha de provas para os crimes sugeridos no ponto 2.1 do presente documento de consulta, a diligência de intercepção de comunicações deverá ter como objecto aquelas que estão em curso.

Quanto às comunicações já concluídas, nomeadamente o conteúdo das comunicações, armazenado no aparelho de comunicações ou no suporte de armazenamento físico (e.g. disco rígido móvel) apreendido nos termos da lei, ou no suporte de armazenamento virtual (e.g. armazenamento em nuvem), se o mesmo for susceptível de se revelar de grande interesse para a descoberta da verdade e deverá ser levado ao conhecimento do juiz. Contudo, para extrair dados de interesse, é sempre necessário desbloquear o aparelho de comunicações ou suporte de armazenamento protegido com encriptação, pelo que se propõe:

(1) Em relação à investigação e à recolha de provas para os crimes sugeridos no ponto 2.1 do presente documento de consulta, quando houver fundadas razões para crer que o conteúdo das comunicações guardado no instrumento de comunicações apreendido, no suporte de armazenamento físico apreendido ou no suporte de armazenamento virtual, seja susceptível de se revelar de grande interesse para a descoberta da verdade, **o juiz pode, por despacho, ordenar** ao proprietário ou possuidor desse instrumento ou suporte que proceda à abertura ou ao desbloqueio do mesmo e que preste auxílio na consulta e recolha dos dados nele guardados;

(2) Se os interessados se recusarem a colaborar ou demorarem sem razão legítima, serão punidos, por crime de desobediência qualificada prevista no n.º 2 do artigo 312.º do Código Penal, com pena de prisão até dois anos ou pena de multa até 240 dias; por outro lado, **o juiz** competente **pode ordenar ou autorizar** a adopção de todos os meios técnicos viáveis para proceder à recolha dos dados guardados nesse aparelho ou suporte;

(3) Sempre que o juiz considerar as informações, recolhidas mediante a referida diligência, como provas importantes, ordena a sua junção aos autos. Caso contrário, será ordenada a sua destruição, ficando todos os indivíduos envolvidos nas operações obrigados ao dever de sigilo relativamente àquilo de que tenham

tomado conhecimento.

3.2 Estabelecimento dos deveres para os operadores de telecomunicações e os prestadores de serviços de comunicações em rede

A execução da intercepção de comunicações pressupõe a colaboração e apoio dos respectivos sectores, pelo que se propõe estabelecer deveres para os "operadores de telecomunicações" e os "prestadores de serviços de comunicações em rede".

Os "operadores de telecomunicações" são as entidades que possuem licença de exploração de serviço de telecomunicações fixo ou móvel e de serviço de acesso à internet.

Os "prestadores de serviços de comunicações em rede", por seu turno, são as entidades que fornecem ou exploram os serviços de comunicações de qualquer tipo, de forma individual ou colectiva, servindo-se, para o efeito, de uma rede de telecomunicações e dos respectivos meios técnicos, designadamente através de aplicações móveis (app), sítios de internet ou programas de computador.

3.2.1 Dever de colaboração

Após legalmente autorizada, a execução da intercepção de comunicações ainda pressupõe a colaboração dos respectivos sectores. As legislações de alguns países e regiões definem que os operadores de telecomunicações e/ou os prestadores de serviços de comunicações em rede têm o dever de colaboração e prestam, nos termos das leis ou ordens legais das autoridades, a colaboração, apoio e informações necessárias, sem demora, aos tribunais, magistrados do Ministério Público e agentes de investigação que exercem funções policiais na aplicação dessas medidas.

Nessa perspectiva, propõe-se que os "operadores de telecomunicações" e os "prestadores de serviços de comunicações em rede" tenham de prestar a colaboração e o apoio técnico necessários à entidade competente, não podendo recusar ou demorar, sem razão legítima, o cumprimento das ordens determinadas, sob pena de incorrer no crime de desobediência qualificada, previsto e punido, no n.º 2 do artigo 312.º do Código Penal, com pena de prisão até 2 anos ou com pena de multa até 240 dias.

3.2.2 Dever de conservação

Os agentes do crime, na sua prática, quando usam os meios de telecomunicações para contactar, comunicar e transmitir informações, podem deixar nas redes de telecomunicações mensagens e outros elementos relevantes para a investigação, sendo possível conservar esses traços naquelas redes. Estas informações podem ajudar a investigação e o trabalho de recolha de provas, pelo que, sendo assim, existe uma grande necessidade de as conservar durante um determinado prazo.

Nesse sentido, propõe-se que:

(1) Os operadores de telecomunicações devam conservar os registos das comunicações produzidos pelos seus serviços, durante 1 ano, na RAEM;

(2) Os prestadores de serviços de comunicações em rede devam conservar os registos das comunicações na RAEM por via da utilização desses serviços, durante 1 ano, na RAEM.

Importa referir que os registos das comunicações conservados não incluem qualquer conteúdo das comunicações, só indicam os dados produzidos pela utilização dos serviços de comunicação. Durante a conservação, os operadores de telecomunicações e os prestadores de serviços de comunicações em rede devem garantir a segurança e o sigilo desses dados.

O incumprimento do dever de conservação, por parte dos operadores das telecomunicações e dos prestadores de serviços de comunicações em rede, será classificado como infracção administrativa. A competência para instaurar o procedimento infraccional e para aplicar as sanções cabe à Polícia Judiciária:

(1) Se o infractor for uma pessoa singular, será sancionada com multa de MOP$20.000 (vinte mil patacas) a MOP$200.000 (duzentas mil patacas);

(2) Se for uma pessoa colectiva, com multa de MOP$150.000 (cento e cinquenta mil patacas) a MOP$500.000 (quinhentas mil patacas).

3.3 Penalização de outros actos irregulares

Para que a medida de intercepção de comunicações seja rigorosamente implementada de acordo com o "Regime Jurídico da Intercepção e Protecção de Comunicações", bem como o conteúdo das comunicações daí recolhido, obtido, conservado e processado seja apenas utilizado para as finalidades admitidas por lei e não haja abusos, propõe-se que a intercepção de comunicações sem ordem ou

autorização do juiz, a violação do dever de sigilo e a utilização indevida das informações obtidas pela intercepção sejam classificadas como crime, e que, se esses actos irregulares não forem punidos com pena mais pesada, de acordo com as disposições de outras leis, sejam punidos com pena de prisão até 3 anos ou com pena de multa, e classificados como crime público, para que os indivíduos encarregados da execução, colaboração ou coordenação na intercepção e os que detêm ou tenham conhecimento do referido conteúdo sejam sujeitos à lei, de forma a garantir os direitos, no que concerne às comunicações dos residentes.

Se uma pessoa colectiva praticar esses actos, deverá assumir as responsabilidades penais. Sugere-se que seja punida com pena de multa de 100 dias a 1.000 dias, num valor diário entre MOP$500 (quinhentas patacas) e MOP$20.000 (vinte mil patacas), e que possam ser aplicadas cumulativamente as penas acessórias, incluindo a privação do direito a subsídios ou subvenções outorgados por serviços ou entidades públicos e a publicação da sentença condenatória.

4. Aplicação subsidiária das disposições do Código de Processo Penal

O presente "Regime Jurídico da Intercepção e Protecção de Comunicações" adopta a forma de lei avulsa. O regime de escutas telefónicas torna-se independente do Código de Processo Penal e, por este motivo, sugere-se que nas matérias que não forem expressamente previstas se apliquem subsidiariamente as disposições do Código de Processo Penal.

5. Data da entrada em vigor

Para que as autoridades judiciais e os diferentes serviços se possam preparar para bem implementar e executar o "Regime Jurídico de Intercepção e Protecção das Comunicações", sugere-se que a presente lei entre em vigor 90 dias após a sua publicação.

Além disso, considerando que o "Regime Jurídico de Intercepção e Protecção das Comunicações" tem uma ligação directa com os actuais "operadores de telecomunicações" e "prestadores de serviços de comunicações em rede", propõe-se que, durante um ano após a entrada em vigor, os "operadores de telecomunicações" e "prestadores de serviços de comunicações em rede" sejam dispensados do dever de conservação, permitindo-lhes fazer os preparativos adequados durante o período de transição.

Extractos das respectivas legislações de outros países e regiões

(As informações deste anexo estão actualizadas até final de Abril de 2018)

Tipos de comunicações que podem ser alvo de intercepção
Portugal Conversações, comunicações, conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e a intercepção de comunicações entre presentes. Referência: artigo 189.º do Código de Processo Penal
Alemanha Telecomunicações referem-se ao processo técnico de emissão, transmissão e recepção de sinais através de dispositivos de telecomunicações. Quando estão reunidos os requisitos legais, as telecomunicações podem ser escutadas e registadas. Quando estão reunidos os requisitos legais, as palavras faladas num contexto não-público, dentro ou fora da habitação, podem ser escutadas e registadas por meios técnicos. Referência: alínea 22) do artigo 3.º da Lei das Telecomunicações, artigos 100.º - A, 100.º - C, e 100.º - F, do Código de Processo Penal
Reino Unido A obtenção de comunicações ou outras informações pode ser feita por: escuta, observação ou audição das comunicações ou outras actividades de uma pessoa; gravação de algo que seja escutado, observado ou ouvido. Referência: artigo 99.º do *Investigatory Power Act 2016*
Estados Unidos da América Autoriza-se a intercepção da comunicação por fio, electrónica e oral. Interceptar significa a aquisição auditiva ou por outra forma, do conteúdo de qualquer comunicação por fio, electrónica ou oral, através do uso de qualquer dispositivo electrónico, mecânico ou outro. Referência: artigo 2510.º do Código dos EUA
O território de Taiwan O termo "comunicações", como usado nesta Lei, significa: 1. Telecomunicações por fio e sem fio que emitem, armazenam, transmitem ou recebem símbolos, escrita, imagens, sons ou outras mensagens, através do uso de equipamentos de telecomunicações; 2. Correio e correspondência escrita; 3. Discurso e conversações. Referência: artigo 3.º da Lei de Protecção e Fiscalização de Comunicações

Meios de intercepção
Portugal A intercepção e a gravação de conversações ou comunicações telefónicas só podem ser autorizadas por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público. Referência: artigo 187.º do Código de Processo Penal
Alemanha Em situações legalmente previstas, a escuta e o registo de telecomunicações podem ser autorizados sem o conhecimento dos indivíduos envolvidos. Referência: artigo 100.º- A do Código de Processo Penal
Reino Unido A obtenção de comunicações ou outras informações pode ser feita por: escuta, observação ou audição das comunicações ou outras actividades de uma pessoa; gravação de algo que seja escutado, observado ou ouvido. Referência: artigo 99.º do *Investigatory Power Act 2016*
Estados Unidos da América Interceptar significa a aquisição auditiva ou por outra forma, do conteúdo de qualquer comunicação por fio, electrónica ou oral através do uso de qualquer dispositivo electrónico, mecânico ou outro. Referência: artigo 2510.º do Código dos EUA
Região Administrativa Especial de Hong Kong Os meios da intercepção incluem *overhearing*, escuta, monitorização, registo e intercepção. Referência: artigo 2.º da *Interception of Communications and Surveillance Ordinance*
O território de Taiwan A fiscalização de comunicações é efectuada através da intercepção, escuta, gravação de som, vídeo, fotografia, abertura, examinação, fotocópia ou outras formas semelhantes e necessárias. Referência: artigo 13.º da Lei de Protecção e Fiscalização de Comunicações

Prazo de duração da intercepção de comunicações
Portugal A intercepção e a gravação de conversações ou comunicações são autorizadas pelo prazo máximo de três meses, renovável por períodos sujeitos ao mesmo limite, desde que se verifiquem os respectivos requisitos de admissibilidade para a intercepção e a gravação. Referência: artigo 187.º do Código de Processo Penal
Alemanha O prazo máximo do mandado é de três meses. Dado que foi obtido o resultado da investigação, uma vez que as condições pressupostas continuem a existir, é autorizada a prorrogação, não devendo exceder três meses de cada vez. Referência: artigo 100.º - E do Código de Processo Penal
Reino Unido Seis meses contados a partir da data da emissão do mandado de intercepção específica, sendo esse prazo renovável. Referência: artigo 32.º do *Investigatory Powers Act 2016*
Austrália Deve-se especificar no mandado o prazo de validade. Este mandado pode ser revogado pelo Procurador-geral a qualquer momento, antes do fim do prazo especificado. O período marcado não pode ser superior a 6 meses salvo os casos que envolvem a segurança nacional. O mandado que tenha sido emitido e outras situações específicas não impedem a emissão de um mandado adicional para os serviços de telecomunicações ou indivíduos. Referência: artigo 9.º - B da Lei de Telecomunicações (Intercepção e Acesso) de 1979
Região Administrativa Especial de Hong Kong Em situações com delegação do juiz e delegação de competências administrativas, o prazo não poderá exceder 3 meses a contar da data de entrada em vigor da delegação em causa; quanto à renovação, não poderá exceder 3 meses a contar da data de entrada em vigor da renovação da mesma. Referência: artigos 10.º, 13.º, 16.º e 19.º da *Interception of Communications and Surveillance Ordinance*

Dever de colaboração para os operadores de telecomunicações e os prestadores de serviços de comunicações em rede
Portugal As empresas que oferecem redes e serviços de comunicações electrónicas podem estar sujeitas na sua actividade, de acordo com a legislação aplicável, à instalação, a expensas próprias, e disponibilização de sistemas de intercepção legal às autoridades nacionais competentes bem como ao fornecimento dos meios de desencriptação ou decifração sempre que ofereçam essas facilidades. Referência: artigo 27.º da Lei das Comunicações Electrónicas, Lei n.º 5/2004
Alemanha Em cumprimento da ordem da monitorização ou do registo de telecomunicações, os agentes que forneçam ou participem nas actividades de telecomunicações devem colaborar com os tribunais, magistrados e pessoal de investigação que exerce funções de polícia na aplicação dessas medidas e, sem demora, na prestação das informações necessárias. Referência: artigo 100.º -A do Código de Processo Penal
Reino Unido O mandado de intercepção específica ou de assistência mútua autoriza qualquer conduta para obter os respectivos dados de sistemas de qualquer operador postal ou de telecomunicações. Referência: artigo 15.º da *Investigatory Powers Act 2016*
Japão A fim da realização da intercepção de comunicações, o magistrado ou o agente da polícia judiciária pode exigir aos fornecedores dos serviços de comunicações a conexão dos dispositivos destinados à intercepção ou a prestação de outra assistência necessária. Neste caso, os fornecedores não podem recusar o pedido sem ter causa legítima. Referência: artigo 11.º da Lei de Fiscalização das Comunicações no Processo de Investigação Criminal
Região Administrativa Especial de Hong Kong Com o propósito de executar a ordem, emitida pelo Chefe do Executivo, relativa à intercepção de qualquer tipo de informação legalmente autorizada, devem-se oferecer facilidades razoáveis e necessárias para essa intercepção. Referência: artigo 33.º da *The Telecommunications Ordinance*

Dever de colaboração para os operadores de telecomunicações e os prestadores de serviços de comunicações em rede
O território de Taiwan As empresas de telecomunicações e as postais estão sujeitas ao dever de colaborar na execução da vigilância das comunicações, podendo o órgão executivo usar os equipamentos dessas empresas destinados à vigilância e requerer a assistência dos seus funcionários. Referência: artigo 14.º da Lei de Protecção e Fiscalização de Comunicações

Registos de comunicações
Portugal Os fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações devem conservar os dados previstos no mesmo artigo pelo período de um ano a contar da data da conclusão da comunicação. Referência: artigo 6.º da Lei n.º 32/2008, Conservação de Dados Gerados ou Tratados no Contexto de Oferta de Serviços de Comunicação Electrónica.
Estados Unidos da América Os fornecedores dos serviços de comunicações electrónicas ou de terminais remotos, devem revelar, aos serviços do governo, os registos de comunicações dos assinantes. Os fornecedores dos serviços de comunicação com fio ou electrónicos ou de terminais remotos devem, de acordo com as exigências do governo, adoptar todas as medidas necessárias para a conservação dos registos ou outros dados que tenham sido processados durante o período do processo judicial ou outros processos equiparáveis. Estes registos devem ser conservados por um período de 90 dias. Mediante nova solicitação por parte do governo, o prazo para a conservação destes dados pode ser prorrogado por outros 90 dias. Referência: artigo 2703.º do Código dos EUA
Austrália Os fornecedores dos serviços de telecomunicações devem conservar, nos termos da lei, por um período de 2 anos, as informações e os documentos em sistemas informáticos, previstos na legislação. Referência: artigo 187.º - C da Lei de Telecomunicações (Intercepção e Acesso) de 1979
República da Coreia Os operadores de serviços de telecomunicação devem conservar durante doze meses os dados relativos à data das comunicações e à hora do início e fim das mesmas, feitas pelos assinantes, aos números das telecomunicações, quer realizadas quer recebidas, aos números dos assinantes da outra parte e à frequência da utilização. Referência: artigo 41.º da Ordem de Implementação da Lei da Protecção do Segredo de Comunicações
O território de Taiwan As autoridades competentes têm o direito de exigir às empresas de telecomunicações a consulta dos registos de comunicações e dos dados de assinantes. No tocante à conservação dos registos de comunicações das empresas de telecomunicações do tipo I: sendo dos últimos 3 meses, para a comunicação efectuada no interior da cidade; sendo dos últimos 6 meses, para a comunicação de longa distância, como a comunicação internacional ou a efectuada no território de Taiwan; sendo também dos últimos 6 meses, para a comunicação efectuada por via de telemóvel. Referência: artigo 7.º da Lei de Telecomunicações, artigo 5.º da Medidas Implementadas por Empresas de Telecomunicações no Tocante à Consulta, por Instituições Relevantes, de Registos de Comunicações

Sanção criminal pelo acto de violação de comunicações
Portugal Quem interceptar, gravar, registar, utilizar, transmitir ou divulgar conversa, comunicação telefónica, mensagem de correio electrónico ou facturação detalhada, é punido com pena de prisão até 1 ano ou com pena de multa até 240 dias. Quem, sem consentimento, se intrometer, tomar conhecimento ou divulgar o conteúdo de telecomunicações, é punido com pena de prisão até 1 ano ou com pena de multa até 240 dias. O funcionário que, sem estar devidamente autorizado, revelar segredo de que tenha tomado conhecimento ou que lhe tenha sido confiado no exercício das suas funções, ou cujo conhecimento lhe tenha sido facilitado pelo cargo que exerce, com intenção de obter, para si ou para outra pessoa, benefício, ou com a consciência de causar prejuízo ao interesse público ou a terceiros, é punido com pena de prisão até 3 anos ou com pena de multa. O funcionário de serviços dos correios, telégrafos, telefones ou telecomunicações que, sem estar devidamente autorizado, tomar conhecimento ou revelar a terceiros o conteúdo das comunicações, em razão das suas funções, é punido com pena de prisão de 6 meses a 3 anos ou com pena de multa não inferior a 60 dias. Referência: artigos 192.º, 194.º, 383.º e 384.º do Código Penal
Alemanha A escuta ilegal é punida com pena de prisão até 3 anos ou pena de multa; e a violação de segredos do discurso de outrem, praticada por funcionários públicos ou por indivíduos que exercem funções públicas especiais é punida com pena de prisão até 5 anos ou com pena de multa. Referência: artigo 201.º do Código Penal
Estados Unidos da América Salvo disposição legal em contrário, quem interceptar dolosamente ou tentar interceptar, ou promover a intercepção ou tentativa de intercepção por terceiros de qualquer comunicação por fio, verbal ou electrónica, deve ser punido com pena de prisão até 5 anos ou com pena de multa, ou as penas aplicadas cumulativamente. Referência: artigo 2511.º do Código dos EUA
Região Administrativa Especial de Hong Kong O funcionário de telecomunicações, ou qualquer pessoa que tem funções relacionadas com os serviços de telecomunicações, embora não seja funcionário de telecomunicações, que intercepta, detém ou atrasa intencionalmente qualquer mensagem; ou qualquer pessoa que danifica, remove ou interfere, de qualquer maneira, em dispositivos de telecomunicações, com a intenção de interceptar ou descobrir o conteúdo de uma mensagem, comete um crime. Uma vez que seja condenado através do processo sumário, é punido com pena de multa de 10.001 a 25.000 de doláres de Hong Kong e com pena de prisão de 2 anos. Referência: artigos 24.º e 27.º da *The Telecommunications Ordinance*

Sanção criminal pelo acto de violação de comunicações
O território de Taiwan A monitorização ilícita de comunicações é punida com pena de prisão até 5 anos; a monitorização ilícita de comunicações, se for efectuada por funcionários públicos ou trabalhadores que executam a monitorização ou que prestam apoio à sua execução, aproveitando-se da sua posição, oportunidade ou meios nas próprias funções ou actividade, é punida com pena de prisão de 6 meses a 5 anos. Referência: artigo 22.º da Lei de Protecção e Fiscalização de Comunicações

Região Administrativa Especial de Macau

Consulta Pública sobre a Proposta do Regime Jurídico da Intercepção e Protecção de Comunicações

Tabela para apresentação de opiniões e sugestões relativas à legislação

Dados básicos
Nome ou designação da entidade:
Declaração de confidencialidade: por favor assinale com o sinal ✓ na quadrícula caso deseje manter a sua opinião ou sugestão confidencial----------☐
Data de entrega: _____(assinatura) _____ /_____ /_____ (dia/mês/ano)

Objecto de discussão	Opinião ou sugestão
2.1 Tipos de crimes aplicáveis	
2.2 Tipos de comunicações que podem ser alvo de intercepção	
2.3 Meios de intercepção	

Objecto de discussão	Opinião ou sugestão
2.4 Prazo de duração da intercepção de comunicações	
2.5.1 Prazo para entrega dos elementos recolhidos durante a intercepção de comunicações	
2.5.2 Data de início para o exame dos autos	
3.1 Consulta e extracção do conteúdo de comunicações armazenado por ordem do juiz	
3.2.1 Dever de colaboração	
3.2.2 Dever de conservação	

Objecto de discussão	Opinião ou sugestão
3.3 Penalização de outros actos irregulares	
5. Data da entrada em vigor	
Outras opiniões ou sugestões	

Observação:

As opiniões ou sugestões podem ser apresentadas através do preenchimento da tabela supra ou por escrito numa folha à parte, **especificando devidamente o número do capítulo e secção aos quais pertencem e respeitando a ordem sequencial dos mesmos**, para facilitar a análise e o acompanhamento.