INSTITUTO
UNIVERSITÁRIO
DE LISBOA

A implementação do Regulamento de Cibersegurança (Cybersecurity Act) e o seu impacto para cibersegurança

Filipa Cristina Pereira Gil

Mestrado em Políticas Públicas

Orientador(a):
Doutora Ana Isabel Xavier, Professora Associada Convidada,
ISCTE - Instituto Universitário de Lisboa

Co-Orientador(a):
Doutora Maria José Sousa, Professora Auxiliar c/ Agregação,
ISCTE - Instituto Universitário de Lisboa

Novembro, 2021

SOCIOLOGIA
E POLÍTICAS PÚBLICAS

Departamento de Ciência Política e Políticas Públicas

A implementação do Regulamento de Cibersegurança (Cybersecurity Act) e o seu impacto para cibersegurança

Filipa Cristina Pereira Gil

Mestrado em Políticas Públicas

Orientador(a):
Doutora Ana Isabel Xavier, Professora Associada Convidada,
ISCTE - Instituto Universitário de Lisboa

Co-Orientador(a):
Doutora Maria José Sousa, Professora Auxiliar c/ Agregação,
ISCTE - Instituto Universitário de Lisboa

Novembro, 2021

Agradecimento

Na elaboração desta dissertação estiveram várias pessoas envolvidas e graças a elas consegui concluir mais uma etapa da minha vida académica. Quero agradecer a todos os alunos do mestrado de políticas públicas com quem pude discutir ideias de temas e conceitos. Também agradeço aos professores que nos deram liberdade de com cada trabalho poder escolher e aprofundar a área de investigação em que nos quisemos focar.

Um agradecimento especial à minha família que me apoiou quando estive a estudar em Lisboa, à minha tia e primos que me fizeram sentir em família. Ao meu pai e à minha mãe por me apoiarem e motivarem em tempo de pandemia para nunca desistir e por darem-me espaço para desabafar e espairecer, sem o seu apoio incondicional nos tempos mais difíceis não teria concluído.

Um agradecimento à família que se escolhe, que são os meus amigos, que aturaram os meus humores de tristeza, pânico e ansiedade, mostrando que os desafios fazem parte da vida e que têm é de ser superados, nunca desistindo. Um especial obrigado aos amigos que leram e deram opinião sobre a minha dissertação e que me responderam às mensagem às tantas da noite.

À minha orientadora Professora Doutora Ana Isabel Xavier, e coorientadora Professora Doutora Maria José Sousa, agradeço pela paciência, amabilidade e disponibilidade, especialmente nas alturas mais importantes em que perdia o meu caminho, estavam sempre lá para me ajudar.

Resumo

A tecnologia tem um papel importante na nossa vida privada, nas empresas e nos Estados a nível global. Dependemos da tecnologia para comunicar, trabalhar, para as atividades sociais, saúde, energia, transportes e para inovar de forma mais ecológica. Desde 1985 que começaram a ser formuladas políticas e iniciativas europeias de cibersegurança, inicialmente como soluções para melhorar a economia, progressivamente, como uma forma de proteger as infraestruturas críticas, e com uma abordagem abrangente e coesa que envolve também cibercriminalidade, inovação tecnológica e ciberdefesa. Tendo em conta o novo regulamento de cibersegurança, que entrou em vigor em 2019, com o objetivo de aumentar o nível de cibersegurança europeu e evitar a fragmentação do mercado interno dos sistemas de certificação diversos, o objetivo desta dissertação é analisar que impactos podemos identificar na sua implementação e quais os contributos para a construção do projeto europeu de cibersegurança para lá de ser apenas uma ferramenta de harmonização do mercado interno. Para tal, iremos utilizar o método de implementação de política de Sabatier e Mazmanian (1983), dado o regulamento de cibersegurança ser de adesão voluntária e dependente de incentivos estatais. O estudo de caso alemão é apresentado como exemplo.

Palavras-chave: Cibersegurança; União Europeia; Certificação; Políticas públicas; Alemanha;

Abstract

Technology has an important role in our private lives, business and states at a global level. We rely on technology to communicate, to work, for social activities, health, energy, transportation and to innovate in a green way. Since 1985 the European Union started to formulate initiatives and cybersecurity policy, in the beginning as a solution to enhance the economy, after was as a way to protect critical infrastructures and as a broad and cohesive way that involves ciber criminality, technological innovation and cyber defense. The creation of the new Cybersecurity Act, which entered into force in 2019, has the objectives of increasing the level of European cybersecurity and to avoid the fragmentation of the European market from the large number of certification schemes. It is the objective of this dissertation to analyze the impacts that the Cybersecurity Act will have in its implementation and what contribution will it have in the construction of the European cybersecurity project and not just being a tool to harmonize the market. For this reason, we will use the policy implementation method from Sabatier and Mazmanian (1983), because the Cybersecurity Act is of voluntary adherence and it depends on national incentives. We also present Germany as a case study example.

Keywords: Cybersecurity; European Union; Certification; Public Policy; Germany.

Índice

Glossário de Siglas

ACF – Advocacy Coalition Framework

BSI – Bundesamt für Sicherheit in der Informationstechnik/ Autoridade Nacional Alemã de Segurança de Informação

CC – Commom Criteria

CCRA – Common Criteria Recognition Agreement

CDT – Cyber Diplomacy Toolbox

CERT – Computer Emergency Response Team

cPPP – Cooperação Parcerias Público-Privadas

CSA – Cybersecurity Act

EDPR – Comité Europeu para a Proteção de Dados

EFTA – Associação Europeia de Comércio Livre

EM – Estados-membros da União Europeia

ENISA – Agência Europeia para a Segurança das Redes e da Informação

GECC – Grupo Europeu para a Certificação de Cibersegurança

I&D – Investigação e desenvolvimento

IdC – Internet das Coisas

NIS – Network and Information Security

OTAN – Organização do Tratado do Atlântico Norte

PEPIC – Programa Europeu de Proteção das Infraestruturas Críticas

PME – Pequenas e Médias Empresas

RAIC – Rede de Alerta para as Infraestruturas Críticas

RGPD – Regulamente Geral sobre a Proteção de Dados

SCCG – Stakeholder Cybersecurity Certification Group

SOG-IS – Seniors Officials Group on Information System Security

TIC – Tecnologias de Informação e Comunicação

URWP – Union Rolling Work Programme

Introdução

A internet e as tecnologias de informação exercem um papel vital na nossa sociedade, tanto na área económica, financeira, informação e comunicação, como em atividades sociais, saúde, energia, transportes, sendo utilizadas por cidadãos, governos e empresas a nível global. Com um aumento exponencial de produtos digitais disponíveis torna-se difícil de acompanhar com medidas de segurança e legislação em conformidade. O número de dispositivos conectados à internet tem vindo a aumentar, com uma estimativa de 25 biliões de dispositivos em 2025, segundo o factsheet *The EU's Cybersecurity Strategy in the Digital Decade*. No entanto, este aumento de conectividade e digitalização leva ao aumento de riscos de cibersegurança em toda a sociedade. A Symantec detetou uma subida de ciberataques de vários tipos[1] em 2019 e em 2020.

De facto, ameaças de ciberataques afetam a estrutura do Estado e o mercado financeiro (Martins 2012) e uma vez que nenhum Estado é imune a esta nova realidade do ciberespaço, tem que se promover uma cooperação global para conseguir estabilidade. A UE desenvolveu vários instrumentos ao longo dos anos para responder às dificuldades e sensibilizar os Estados-Membros (EM) para o tópico de cibersegurança. A política europeia de cibersegurança é fragmentada e diferenciada temporalmente em três áreas – cibercrime, ciberdefesa, segurança de redes e informação, cada um com mandatos institucionais, processos e lógicas diferentes (Christou 2018). Nesta dissertação vamos analisar apenas a área de segurança de redes e informação e infraestruturas crítica, onde se insere o regulamento de cibersegurança (Cybersecurity Act).

Com o objetivo de analisar que impacto a implementação deste regulamento vai ter no reforço de cibersegurança, iremos descrever e analisar no primeiro capítulo as políticas europeias de cibersegurança para refletir sobre os progresso feito até agora. No segundo capítulo, fazemos uma análise do regulamento de cibersegurança, evidenciando as mudanças e suas repercussões. No terceiro capítulo, identificamos as causas e os objetivos para a criação do regulamento de cibersegurança e de como ele vai ser implementado, dando como exemplo a Alemanha e utilizando o modelo de implementação política de Sabatier e Mazmanian (1983).

[1] Subida de 56% de ataques por web, subida de 33% de ataques por ransonware, 78% de ataques na rede de fornecimento. Em 2020 subiu o número de emails maliciosos, aumento de phishing e ataques de IdC.

No quarto e último capítulo, tiramos as conclusões e perspetivamos como o regulamento de cibersegurança influencia a atuação da UE no ciberespaço.

Definição de Conceitos

Universalmente não há uma definição aceite que capture as várias dimensões de cibersegurança (Craigen et al 2014, Weber e Studer 2016), impedindo assim o avanço tecnológico e científico, aumentando a predominância técnica e separando disciplinas que deviam atuar em conjunto para resolver os desafios complexos de cibersegurança. Existem vários autores que definem cibersegurança de forma abrangente – Cavelty (2010) e Canongia & Mandarino (2014) definem a cibersegurança como forma de assegurar a continuidade da sociedade de informação, protegendo as suas estruturas, a informação, os dispositivos e software através de medidas técnicas e não técnicas. Os autores Craigen et al (2014) acrescentam que para assegurar a continuidade, é necessário proteger o ciberespaço de ocorrências malignas que deturpem a sua atividade, juntamente com os direitos e a propriedade dos utilizadores. De opinião diferente, mas também abrangente, Barrinha (2020) define a utilização do termo cibersegurança como uma tentativa de os políticos traduzirem a complexidade e a importância da tecnologia no mundo atual.

Alguns autores definem cibersegurança de forma técnica e restrita. ITU (2009) define cibersegurança como um conjunto de ferramentas políticas e de segurança, uma gestão de risco e treino utilizado para proteger o ciberespaço, organizações e utilizadores. Bayuk (2010) utiliza esta definição e vai mais longe, define o objetivo de cibersegurança que se quer obter, considerando a escolha das ferramentas. Exemplifica que para aumentar a resiliência é necessário incluir todos os elementos para conseguir segurança, utilizando programas como antivírus e *firewall*, sensibilizar os utilizadores para as ameaças existentes e por último cibersegurança da informação. Seguindo essa lógica, autores como Kemmerer (2003) e Schatz (2017) definem cibersegurança como métodos defensivos (antivírus, *firewall*) para proteger e detetar possíveis criminosos. Esta definição de cibersegurança como forma de combate, deteção de crimes ou ataques maliciosos é compartilhada por Amoroso (2006), Public Safety Canada (2014) e o Comité EUA de Sistemas de segurança (2014).

Podemos separar os discursos existentes em técnicos, em contexto de práticas de segurança relacionadas com a combinação de ações ofensivas e defensivas (Schatz 2017), e abrangentes

que incluem todas as áreas no conceito de cibersegurança por serem um termo complexo que envolve interação entre humanos e sistemas (Craigen et al 2014).

Consequentemente, segundo Cavelty (2015), a discussão sobre cibersegurança sempre foi e estará influenciada pela revolução de informação, pelo que a definição nunca será estática porque os aspetos técnicos também estão em constante evolução.

CAPÍTULO 1

União Europeia como ator no ciber espaço

Com a intenção de identificar políticas europeias de cibersegurança que conduziram à criação de um esquema de certificação europeu, torna-se necessária uma contextualização histórica das políticas de cibersegurança. Começamos por nomear os objetivos da União Europeia presentes no Tratado de Lisboa[2] e na Carta dos Direitos Fundamentais da EU que são de "promover a paz, os seus valores e o bem-estar dos seus cidadãos", "garantir a liberdade, a segurança e a justiça, sem fronteiras internas" e por último, "promover o progresso científico e tecnológico", sendo a tecnologia associada ao progresso e o ciberespaço um novo território com novos perigos. Segundo a comunicação de 2013 (JOIN/2013/01 final) trata-se de uma iniciativa da UE de passar os mesmos valores e normas aplicados no dia a dia para o ciberespaço (Dewar 2017): a abertura e liberdade no uso da internet, estabelecer normas de conduta, aplicação do direito internacional no ciberespaço, promoção da redução da clivagem digital e construção de uma capacidade de cibersegurança.

1.1. A tecnologia na construção do mercado 1985-2001

As competências da UE desde a sua criação foram de foro económico, com a preparação da formação do mercado comum (Dewar 2017 e Chsristou 2018). As telecomunicações e tecnologia de informação foram identificadas como áreas de necessidade de harmonização, redução de obstáculos à inovação e desenvolvimentos económico, na comunicação de 1985 (COM 85 310 final), de forma a tornarem-se um complemento para o mercado comum na distribuição de produtos, processamento de informação e criação de postos de trabalho. Também com o relatório de 1993 "Growth, Competitiveness, and Employment. The Challenges and Ways Forward into the 21st Century*"* da Comissão, no ponto 3.6 telecommunication networks: creations of new markets, as tecnologias de informação para a economia e para o desenvolvimento do mercado único europeu, são reconhecidas como essenciais para a criação de uma área comum de partilha de informação e uma rede transeuropeia, utilizando a economia como um impulsionador da inovação tecnológica.

[2] Tratado de Lisboa, Artigo 3.º

A UE continuou a desenvolver novas maneiras de implementar um espaço tecnológico europeu. O relatório de Bangemann (1994) foi pedido pelo Conselho com o objetivo de analisar as implicações económicas das novas infraestruturas digitais de telecomunicações e a necessidade da UE se adaptar como forma de ter uma vantagem económica. As escolhas políticas deste relatório tornaram-se as futuras ciber políticas (Dewar 2017): TIC como fundamental para a economia, a proteção dos direitos fundamentais, a proteção de informação e privacidade, a proteção de direitos de autor e combate ao cibercrime. Este relatório estabelece que, para que estes objetivos se concretizem, será necessária cooperação entre atores nacionais e privados. Depois deste relatório, a Comissão lançou duas propostas em 1992 (COM (92) 24 Final) para a proteção de base de dados de computadores e proteção de pessoas singulares sobre os seus dados e a livre circulação dos mesmos.

Nestes primeiros anos a resposta da UE para ciberataques é interpretada como uma ameaça à funcionalidade do mercado único, tal é evidente na comunicação de 1996 (COM (96) 487) onde são enumeradas ameaças[3] com repercussões para o mercado, seguindo o interesse internacional em crimes relacionados com computadores (Carrapiço e Barrinha 2017).

1.2. Proteção de infraestruturas críticas 2001-2010

A cibersegurança não se tornou uma prioridade na agenda europeia até meados dos anos 2000, devido a ameaças[4] presentes nesses anos que facilitaram uma transição da vulnerabilidade percecionada, suplementando a lógica económica, para uma abordagem de segurança na estratégia de cibersegurança europeia (Christou 2018). Essa mudança de raciocínio de segurança refletiu-se na retórica europeia, que se preocupou com conteúdo ilegal, crimes através de computadores e de sensibilizar os EM para a existência deste novo tipo de crimes. A criação do plano eEurope 2002 tinha como objetivo fomentar uma internet mais segura, dentro dos domínios técnicos e políticos, e uma economia dinâmica com base no conhecimento. Também se destacou a importância de proteger infraestruturas de informação, mantendo a importância dada à economia pela UE no ciberespaço e uma estratégia da UE para sensibilizar os EM para o crescente cibercrime.

Com o pressuposto que a economia, a indústria e o modo de vida estavam dependentes de sistemas de informação, comunicação e tecnologia, sendo vulneráveis a ataques exteriores, foi

[3] As ameaças referidas são a violação dos direitos de autor, invasão de privacidade, fraudes de crédito, pornografia infantil e disseminação de ideais racistas.
[4] Surgimento de mais malware de forma consistente, como por exemplo i love you 2000, code red e nimda 2001, blaster e slammer 2003, sasser 2004, zeus 2007, conficker 2008

seguido o modelo americano de proteção de infraestruturas desde a *Presidential Comission* de 1997 (Cavelty 2015), reconhecendo que o crime organizado e terrorismo representam uma ameaça à sociedade de informação. De facto, poderiam paralisar o funcionamento de infraestruturas essenciais, que estavam a ser postas em causa devido a diferenças e insuficiências nacionais (Carrapiço e Barrinha 2017). Assim, as respostas a nível nacional foram vistas como insuficientes para lidar com esta nova ameaça transnacional e uma resposta comum europeia foi introduzida como necessária (Decisão Conselho da União Europeia 2005). Com a comunicação de 2004 (COM (2004) 702 final), a UE começou a ter em vista outros fatores, como a proteção de infraestruturas e sua definição, num esforço de cooperação. Neste sentido, a União Europeia define "infraestruturas críticas" como uma estrutura física de serviços de informação e tecnologia em rede que se for interrompida ou destruída teria um grande impacto na saúde, segurança, economia e no bem-estar da população em geral ou até mesmo no funcionamento do governo. As infraestruturas críticas são de vários setores (economia, finanças, transportes, energia, tecnologia de comunicação e informação, alimentação, saúde, água, administração, produção, armazenamento e transporte de mercadorias perigosas). Podem até nem ser infraestruturas, mas um intermediário numa rede que, caso pare, impossibilita a contínua produção. Estas infraestruturas por serem públicas e/ou privadas requerem uma cooperação entre público e privado, donos e operadores, EM e UE para o contínuo funcionamento e disponibilização de recursos. Na mesma comunicação propõem o Programa Europeu de Proteção das Infraestruturas Críticas (PEPIC), com o objetivo de melhorar a proteção de infraestruturas críticas europeias ao identificá-las e ao estabelecer *working groups* para suportar os EM (Klimburg 2011). Para além disso, PEPIC também é importante para um reforço da segurança coletiva e da cooperação entre atores (Christou 2018). Em 2006 (COM (2006)786 final) é criada a Rede de Alerta para as Infraestruturas Críticas (RAIC) e em 2008 é criada a Diretiva de Proteção de Infraestruturas Críticas que identificou o setor energético e de transporte como essenciais.

A criação da ENISA (Regulation (EC) No 460/2004) foi um resultado de um aumento de sensibilização para a vulnerabilidade que as infraestruturas críticas sofrem e para a importância desses sistemas para a economia e o desenvolvimento social da UE. Porém, segundo Christou (2019) a causa para a sua criação foi devido ao aumento de ciberataques que causaram um dano económico substancial, consequentemente diminuindo a confiança no mercado e os planos de estabelecer um mercado digital. Logo, a perceção do aumento de risco induziu uma resposta de

securitização[5] pelos atores institucionais europeus e aceite pelos EM. Em 2004, foi criada a ENISA com o objetivo de aumentar as capacidades da UE em cibersegurança, auxiliar os EM e o privado na investigação, inovação e desenvolvimento de medidas de prevenção, responder a problemas de segurança de redes de informação e ajudar no funcionamento do mercado interno. O princípio de subsidiariedade delimita as competências e restringe as ações da ENISA como facilitadora, excluindo uma intervenção em ciberdefesa (uma vez que está ao encargo dos Estados) e o cibercrime, que está ao encargo da Europol. As funções da ENISA são facilitar a cooperação para pesquisa e desenvolvimento de políticas europeias, fomentar a cooperação voluntária do público e privado, sensibilizar órgãos públicos e atores importantes da comunidade, partilhar informação e melhores práticas e publicar artigos online de livre acesso. A ENISA facilita a cooperação através de projetos em conjuntos com atores europeus e não europeus (OTAN) ao elaborar exercícios operacionais de simulação de ameaças (Cyber Europe e Cyber Atlantic) de maneira a facilitar a interoperacionalidade. O papel operacional da ENISA nas CERT (Computer Emergency Response Teams), especialmente na EU-CERT, é realizar atividades regulares de estandardização de processos e coordenação dos trabalhos das CERT nacionais.

Em 2006, foi formalizada a primeira estratégia na área de cibersegurança (SSIS) (COM (2006) 251) para uma sociedade de informação segura, que vai para além do mercado e cibercrime para incluir defesa dos direitos fundamentais (privacidade) e a necessidade de proteger infraestruturas críticas. Nesta estratégia a UE estabelece um esquema onde inclui todos os atores envolvidos na área de cibersegurança para que, em conjunto, estabeleçam requisitos mínimos de segurança para as infraestruturas, fomentando um ambiente de parcerias e inclusão com o privado. Esta estratégia é uma abordagem por múltiplos atores, promovendo a cooperação numa segurança coletiva como solução para os sintomas e causas de cibercrime a nível individual e institucional (Christou 2018). Uma vez que são propostas de forma voluntária, os atores codificam as suas próprias responsabilidades, enquanto a UE como facilitadora, disponibiliza informação para tomarem decisões de forma adequada. Segundo Klimburg e Tiirmaa-Klaar (2011) o progresso na área das infraestruturas críticas não foi uniforme, uma vez que alguns EM estão mais avançados que outros. Posto isto, seriam necessárias iniciativas europeias para realocar recursos e desenvolver uma estratégia de cibersegurança de desenvolvimento diferenciado.

[5] Securitização é a transformação de assuntos em matérias de segurança pelos atores políticos, que argumentam o aumento da ameaça para poderem ter recursos ou criar políticas.

2007 e 2008 foram períodos de crise que afetaram a área política de cibersegurança onde aumentou o interesse na proteção do ciberespaço (Dewar 2017). Em 2007 na Estónia, durante protestos públicos, o Parlamento, os media, bancos e outros serviços administrativos foram atacados com DDoS[6], tornando os websites governamentais indisponíveis. O setor bancário ficou inacessível durante quatro horas. O ciberataque demonstrou as fraquezas nas infraestruturas nacionais digitais e os efeitos em cascata que afetaram a área económica e a comunicação por estarem interligadas. Em seguida, em 2008, uma crise financeira começou nos EUA e fez-se sentir na Europa e, como resposta, foi identificado o setor TIC como uma área de investimento para sair da crise financeira e, ao mesmo tempo, assegurar a resiliência do mercado digital, com o objetivo de aumentar o uso de tecnologia digital em todos os setores e tornar a economia europeia com base no conhecimento.

Estes períodos de crise iniciaram um novo processo de segurança pela Comissão Europeia com o apoio dos EM. Em 2009, propostas (Directive 2009/ 140/EC) de rever o Regulamento Europeu de Comunicações Eletrónicas tornaram obrigatório reportar qualquer incidente em redes de informação à autoridade reguladora nacional[7]. A ENISA auxilia os EM a implementar esta nova forma de reportar incidentes, o que proporcionou um avanço de medidas voluntárias para uma segurança coletiva com maior comunicação dos EM com ENISA e redes CERT.

1.3. Uma abordagem abrangente e vinculativa 2010-2017

A autora Tiirmaa-Klaar (2018) denomina de "*cyber awakening*" o período de 2010 a 2013 em que a sociedade e os políticos percecionam a gravidade da cibersegurança. Também denomina EU-CSS 2013 a primeira estratégia compreensiva de cibersegurança europeia, por ser uma cooperação entre a Comissão Europeia e do Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança, "demonstrando a habilidade europeia de trabalhar de uma maneira institucional". Considera-se ainda que assinala uma transição para uma postura assertiva e regulativa da UE em cibersegurança com instrumentos juridicamente vinculativos (Geraldes 2019).

A Estratégia de Cibersegurança da União Europeia 2013 (EU-CSS no JOIN (2013) 1 final) foi proposta pela Direção Geral Connect, com o objetivo de acompanhar o aparecimento de ciberameaças mais avançadas, presente na proposta de 2011 da Comissão. Ademais, uma resposta nacional não é suficiente devido à complexidade do problema, ao grande número de

[6] DDoS, Distributed Denial of Service, é uma tentativa de sobrecarregar o servidor ou um computador, utilizando todos os recursos disponíveis e impossibilitando o seu uso pelo utilizador.
[7] Directive 2009/ 140/EC, artigo 13.º a

atores envolvidos e ciberameaças além-fronteiras, sendo necessária uma cooperação a nível europeu coerente entre os EM (Christou 2018). Uma maior perceção dos riscos demonstrou uma necessidade de maior coerência entre as várias políticas setoriais europeias (Carrapiço e Barrinha 2017), sucedendo na EUCSS uma junção de vários setores.

A EUCSS 2013 é o primeiro documento que aborda infraestruturas críticas, cibercrime e ciberdefesa em conjunto. Na EUCSS, a UE pretende reforçar a cibersegurança, ao melhorar as capacidades tecnológicas tornando-as acessíveis aos Estados, ao aumentar a resiliência das infraestruturas críticas, redes e serviços, diminuindo a cibercriminalidade, garantindo a integridade dos dados através de políticas de armazenamento de dados, I&D industrial e de tecnologia, estabelecendo uma política para o ciberespaço coerente que promova os valores europeus, estabelecendo a estratégia europeia a nível internacional de proteção de uma internet livre e aberta, e promovendo normas e leis internacionais de comportamento estatal no ciberespaço (Tiirmaa-Klaar 2018). Além disso, é necessário integrar as questões cibernéticas na cooperação política, operacional e técnica, através de análise e gestão das crises cibernéticas e partilha de informação sobre as ameaças.

Ademais, a EUCSS consegue estabelecer um mercado interno digital de produtos e serviços europeus de forma a assegurar a competitividade do mercado tecnológico europeu e da segurança das infraestruturas, transmitindo confiança nos produtos europeus ao incentivar o desenvolvimento de recursos industriais e tecnológicos. A Agenda Digital vai de encontro da EUCSS 2013 para desenvolver recursos industriais e tecnológicos em cibersegurança, sendo a Agenda Digital para a Europa 2010 (COM (2010)245 final) uma das sete iniciativas da estratégia Europa 2020. Esta Agenda define o papel importante que as TIC desempenham na economia e sociedade, com medidas para aumentar o acesso à internet, convergência de serviços e a acessibilidade de informação em qualquer dispositivo, aumentar a confiança no mercado que foi fragilizada devido a cibercrime, aumentar o investimento em I&D e aumentar a literacia digital.

No seguimento da estratégia económica de interligar tecnologia e também transmitir confiança no mercado digital europeu, protegendo os direitos dos cidadãos, a sua privacidade e investir em I&D europeu, foi criada a Agenda de Mercado Digital Comum (COM/2015/0192 final). O ponto 3.4 refere como as ciberameaças são um problema para a economia e para os direitos fundamentais dos cidadãos. Esta estratégia reflete o desejo europeu de assegurar a viabilidade económica do mercado europeu pela competitividade, em que as infraestruturas europeias dependem demasiado de operadores privados e estrangeiros para componentes e software (Dewar 2017). Para transmitir segurança e promover o mercado único de produtos

TIC, será um contributo elevar o nível de segurança na UE e a melhorar a economia ao incorporar requisitos de segurança em toda a cadeia de valor dos produtos utilizados. Para atingir este objetivo é necessário incentivar o setor privado a cooperar e estabelecer standards de novas tecnologias, aumentando a sua interoperabilidade e orientando o seu desenvolvimento de forma segura. A Agenda Digital dá como exemplo de áreas de intervenção as comunicações 5G, indústria 4.0, computação de nuvem (cloud), cibersegurança, saúde em linha e Internet das Coisas[8].

Dentro das medidas para melhorar o mercado através de cibersegurança, a Comunicação COM (2016) 410 "Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry", foi a primeira que apresentou um quadro de certificação para a cibersegurança de produtos e serviços TIC, com o objetivo de aumentar a confiança e a segurança em produtos europeus e harmonizar de certificação em todos os EM, tendo em conta vários níveis de cibersegurança (empresas, infraestruturas e consumidor). Para além disso, a certificação surge como uma solução para a proteção de informação, com o potencial de influenciar a indústria para aderir às iniciativas europeias (Kamara 2020).

A comunicação de 2011 (COM (2011) 163 final) pondera os resultados sobre a proteção das infraestruturas críticas da informação e conclui que as abordagens nacionais aos desafios de segurança não são suficientes e que a UE devia desenvolver esforços coletivos de cibersegurança. Em 2013, avança a proposta para garantir um elevado nível comum de segurança das redes de informação na UE, (COM (2013) 48 final) relacionada com a EUCSS. São identificadas insuficiências de segurança na abordagem voluntária europeia, os diferentes níveis de capacidades dos EM e a falta de um mecanismo de cooperação e partilha de informação sobre acidentes. Este documento foi proposto em 2013, mas só entrou em vigor em 2016, tornando-se a diretiva NIS (Diretiva (UE) 2016/1148), que propõe um nível mínimo de capacidades nacionais, fomentando uma cultura de gestão de risco e partilha de informação no público e privado. Também requer que todos os EM tenham uma autoridade nacional de cibersegurança e um órgão para CERT, que receba as notificações de incidentes e prestem assistência na gestão de risco. Apesar de todos os EM terem estratégias de cibersegurança, os níveis de maturidade variam (Klimburg e Tiirmaa-Klaar 2011), e não existem medidas para ultrapassar a fragmentação de capacidades entre Estados (Kammel 2018). As medidas variam, porque para implementar a diretiva NIS é necessário conhecimento técnico devido à complexidade dos procedimentos e para monitorizar a sua aplicação (Markopoulou et al 2019).

[8] Agenda de Mercado Digital Comum 2015, ponto 4.2

Os autores Liveri, Sarri e Darra (2018) dizem que deve ser definido um mínimo de medidas de segurança que deve ter em conta os diferentes níveis de maturidade dos atores envolvidos, as diferentes capacidades operacionais e os padrões diferentes existentes nos setores. Para Markopoulou et al (2019) é favorável que existam divergências entre EM na implementação, aplicando a diretiva consoante as suas características nacionais, o que vai contribuir para uma aplicação efetiva.

A Diretiva quis fomentar uma cultura de gestão de risco e partilha de informação no público e privado, sendo o alvo desta diretiva os operadores de serviços essenciais[9] para a manutenção de infraestruturas críticas. Uma parte importante desta diretiva é que torna obrigatório submeter informação sobre incidentes de impacto significante[10], que são definidos como ataques que impeçam a continuidade de serviços, e encoraja o uso de standards internacionais[11] relevantes para a segurança de redes e sistemas de informação. Ao seguirem esses standards, demonstram uma conduta responsável e de acordo com as regras estabelecidas. Markopoulou et al (2019) identificaram que a diretiva NIS tem medidas mais leves para provedores de serviços digitais, que são livres para tomarem medidas que consideram apropriadas para a gestão de risco dos seus sistemas. A justificação dada foi que teriam mais liberdade de conduzir os seus negócios. Portanto, deixa em dúvida como se podem aplicar medidas de segurança em condições especiais. A diretiva diz que devem ser estabelecidas contratualmente entre o EM e a empresa, porém, os EM não devem impor mais medidas a provedores de serviço, apenas em infraestruturas críticas (Markopoulou et al 2019).

1.4. Um novo pacote de medidas de cibersegurança 2017 – atualidade

Há uma mudança de perspetiva de segurança, que advém da perceção de que crime organizado e terrorismo são uma ameaça para a sociedade de informação e que estava a ser posta em risco devido à falta de coerência legislativa entre Estados Membros (Carrapiço e Barrinha 2017) e que demonstrou o nível nacional como insuficientemente equipado para lidar com esta nova ameaça, sendo necessário uma resolução conjunta motivada pela UE.

[9] Um dos objetivos no artigo 1.º, ponto 2 alínea d) Estabelece requisitos de segurança e de notificação para os operadores de serviços essenciais e para os prestadores de serviços digitais.
[10] No artigo 16-º ponto 3, Os Estados-Membros asseguram que os prestadores de serviços digitais notifiquem a autoridade competente ou a CSIRT, sem demora injustificada, dos incidentes com impacto substancial na prestação dos serviços referidos no anexo III por si oferecidos na União.
[11] No artigo 19.º ponto 1, (…) os Estados-Membros incentivam, sem imposição ou discriminação em favor da utilização de um determinado tipo de tecnologia, a utilização de normas e especificações europeias ou internacionalmente aceites plicáveis à segurança das redes e dos sistemas de informação.

Em 2017, o Presidente da Comissão propôs um pacote de medidas de cibersegurança, durante o discurso de Estado da União, que tinham como objetivo aumentar a resiliência europeia a ciberataques, criar uma resposta legal e efetiva a cibercrimes, e melhorar a estabilidade global através de cooperação internacional. Houve o surgimento de novas ciberameaças com a possibilidade de executar ataques de grande escala (por exemplo, os *ransonwares*[12] globais *WannaCry* e *NotPetya*) e o aparecimento de novas tecnologias (por exemplo IdC) que demonstraram a fácil disseminação de ciberataques em vários setores e o uso de táticas operacionais para influenciar o processo democrático (desinformação). Por conseguinte, em 2017, a UE lançou um pacote de iniciativas legislativas para responder aos novos desafios e uma revisão da EUCSS (JOIN/2017/0450 final), que dá foco à resposta dos EM em caso de ciber incidentes internacionais, referindo a necessidade de maior cooperação entre civil e militar. No pacote, foram criados vários mecanismos como a *blueprint*, uma forma de resposta operacional a ataques de larga escala com mecanismos de cooperação entre EM e instituições europeias. Também foi criada a Cyber Diplomacy Toolbox (CDT) com a intenção de ter capacidade de reação a nível europeu e estatal para influenciar o comportamento de potenciais agressores e ser um instrumento de política externa. Utiliza sanções como uma resposta a criminosos que operaram para além do alcance das agências políticas porque quando a UE impõe sanções, outros países seguem o seu exemplo, como os membros da EFTA, candidatos a UE e países vizinhos (Monet e Pawlak 2017). A opinião da Comissão, no JOIN/2017/0450 final, diz que cibersegurança deve ser baseada em resiliência (aplicar NIS, com suporte de ENISA, mercado digital, centros competência de investigação), dissuasão (atribuição, legislação cibercrime, resposta a ciber incidentes, cooperação público-privada) e cooperação internacional. Bendiek et al (2017) apontam que no novo pacote de medidas de 2017 não há nenhuma solução para fragmentação institucional, há pouco financiamento e força legal nos regulamentos. Assim, como solução, sugerem o fortalecimento da ENISA com a base legal para trabalhar com certificação e supervisionar a implementação de legislação europeia, com mais poder de liderança em soluções operativas, tornando-se "*one stop shop for handling acute cyber attacks*", e aumentar a cooperação com o EC3 e outros atores relevantes.

[12] Ransomware é um software de extorsão que pode bloquear o seu computador e depois exigir um resgate para desbloqueá-lo, definição da Kaspersky.

No Cybersecurity Act há esse fortalecimento, com uma extensão definitiva da ENISA, um aumento no orçamento e a criação de um esquema de certificação, como forma de estabelecer um mercado único de cibersegurança (ponto 2.2 no JOIN/2017/0450 final). A ENISA tem tido um papel importante na ligação entre EM e UE, ajudando a definir planos nacionais das várias diretivas europeias. A rede de certificação de produtos e/ou serviços é uma forma de assegurar uma *security by design* na criação de produtos TIC e pequenos elementos na rede IdC, uma vez que a ameaça cibernética não é uma questão de se vai acontecer, mas de quando vai acontecer.

Em relatórios de ENISA de 2017 sobre a certificação, ela é considerada uma atividade de conformidade, intercetando com a diretiva NIS e com o Regulamento Geral sobre a Proteção de Dados (RGPD). O RGPD marcou uma mudança no panorama de privacidade europeu (Felkner, et al 2020), com vinculação legal para todos os EM, obtendo um maior nível de harmonização. O RGPD contacta com temas de privacidade, proteção de informação e cibersegurança, mas também vai para além disso ao ser um direito fundamental[13]. O RGPD incentiva a criação de esquemas de certificação[14] como uma forma de disseminação de boas práticas em privacidade e proteção de dados em todos os setores dentro da Europa. O RGPD também faculta alguns requisitos para os atores terem em conta quando criam esquemas de certificação, sendo que tem de ser voluntário[15]. Para além disso, os critérios de certificação são estabelecidos por Comité Europeu para a Proteção de Dados (EDPR), necessitando uma renovação ao fim de três anos[16] e um registo publicamente disponível de todas as certificações aprovadas. No entanto, estes certificados não diminuem a responsabilidade de seguir as obrigações legais nem supõem um meio de conformidade legal (Kamara 2020).

Com a pandemia covid, o aumento do uso de teletrabalho, ensino à distância e maior uso dos serviços digitais aumentaram a exposição a ciberataques com novos utilizadores a serem expostos a perigos sobre o qual não tem conhecimento (Nyikes 2021). Como parte do Plano de Recuperação Europeu, a comissão comunicou uma nova estratégia de cibersegurança, COM(2020) 456 final. A estratégia foca-se em três pilares. O primeiro é resiliência e soberania tecnológica, que inclui uma atualização da diretiva NIS, criação de centros operacionais em toda a europa para aumentar a partilha de informação sobre ciberameaças, criação de *hub* de inovação digital para apoiar PMEs, utilização de infraestruturas de comunicação quantum como uma nova forma de transmitir informação confidencial, a criação do European Cyber Shield,

[13] Carta dos Direitos Fundamentais da UE, artigo 8º
[14] RGPD, artigo 42.º certificação, ponto 1
[15] RGPD, artigo 42.º ponto 3
[16] RGPD, artigo 42.º ponto 7

uma rede de centros operações de segurança que usam inteligência artificial para detetar ciberataques e tomam medidas preventivas, implementação da EU 5G Toolbox, uma abordagem com base no risco da segurança de 5G, investir no formação e na I&D e adotar o primeiro programa para o Cybersecurity Act. A reforma da diretiva NIS ou NIS2 vai aumentar os setores abrangidos, que são o espaço, gestão de resíduos, produção de alimentos, hospitais, redes ferroviárias, centros de informação, laboratórios de investigação, produção de matérias médicos, administração pública, correios e serviços de entrega. Além disso, o objetivo de aumentar a resiliência de setores críticos do público e do privado com a revisão NIS2 também vai aumentar os requisitos de segurança impostos nas empresas de grande e média dimensão (incluindo a segurança da cadeia de abastecimento), aplicar políticas de proteção de informação, harmonizar o regime de sanções entre EM, criar a organização (EU CycLONE) como elo para suportar a gestão de crises e incidentes em grande escala, aumentar a partilha de informação entre EM e o papel do Grupo de Cooperação. A NIS2 traz uma nova tarefa para ENISA, um registo de vulnerabilidades europeu.

O segundo pilar, definido pelas capacidades operacionais para prevenir, dissuadir e responder a ciberameaças, propõe estabelecer a Joint Cyber Unit, implementar a agenda de combate ao cibercrime de acordo com a Estratégia de Segurança da União e reforçar o uso da Cyber Diplomacy Toolbox. O terceiro pilar pretende avançar com um ciberespaço segundo os valores europeus, em que a UE promove um ciberespaço global, aberto, estável e seguro com lei internacional, direitos humanos, liberdades fundamentais e valores democráticos. Divulga guias práticos de como aplicar os direitos humanos e liberdades fundamentais no ciberespaço, promove a convenção de Budapeste contra o cibercrime[17] e reforça a partilha de informação na comunidade internacional.

Em ligação com o Programa de Recuperação Europeu e o Green Deal, indo de encontro aos objetivos europeus de uma transição ecológica e transformação digital, foi criado o programa europeu de financiamento chamado Programa Europa Digital, que opera em cinco temáticas: supercomputação, inteligência artificial, cibersegurança, competências digitais avançadas e consolidação de uma utilização ampla de TIC na sociedade e economia. Este programa foi criado com o objetivo de financiar I&D tecnológicos reforçando a resiliência e autonomia digital europeia e recuperando a economia afetada pela pandemia. Ainda mais,

[17] A convenção sobre o cibercrime adotada em Budapeste em 2001 é de cooperação internacional e auxílio jurídico mútuo em questões de cibercrime, harmonização de definições do que constitui um cibercrime (exemplo burla informática, direitos de autor e crime coletivo). Foi criada com o objetivo de combater crime informáticos facilitando a deteção, investigação e o procedimento criminal a nível nacional e internacional.

dentro da temática de cibersegurança, os objetivos são de resiliência, soberania tecnológica e liderança europeia. Disponibiliza orçamento para ações relacionadas com o European Cyber Shield de forma a proteger os cidadãos, a indústria e os valores, capacitar os centros operacionais para melhor cooperação e sensibilização (saúde, resiliência, inovação, 5G) e implementar legislação europeia (NIS e testar capacidades de certificação) e programas assistentes como a avaliação e revisão de propostas.

Em conclusão, a estratégia europeia em cibersegurança foi um projeto incrementalista de políticas públicas e cumulativo de eventos, ganhando força e velocidade com a evolução de ameaças exteriores que trazem para a perceção do público como a cibersegurança é importante na sociedade, economia e indústria (Christou 2018). A UE iniciou o processo político de forma económica e como resposta a cibercrimes que deixaram as infraestruturas vulneráveis. Consequentemente, a UE começou e continua a desenvolver ferramentas e medidas para a sua proteção. Portanto, tornou-se num ator de cibersegurança em forma de segurança coletiva entre EM, onde há uma coordenação institucional e um entendimento mútuo de definições e atuação no ciberespaço (Carrapiço e Barrinha 2017). A securitização coletiva permitiu à UE ter uma nova forma de intervenção, com o RGPD, onde há um balanço da proteção de informação e o livre movimento de informação no mercado, e com o Cybersecurity Act, tendo o esquema de certificação cria um balanço entre proteção de consumidor e competitividade de mercado. Ao regular como os produtos devem ser desenvolvidos e utilizados, com base em princípios humanos, legitimidade democrática e balanço de interesses dos participantes, a UE consegue exercer a sua soberania digital através do mercado (Bendiek e Schallbruch 2019). Estas duas iniciativas aumentaram as capacidades digitais europeias e deram ao cidadão controlo sobre os seus dados pessoais. As iniciativas deram base à ideia de soberania europeia, em que a UE é líder em definir standards de atividades online para salvaguardar os seus cidadãos, com uma abordagem ética para os desafios digitais (Liaropoulos, A. 2021).

CAPÍTULO 2

Regulamento de Cibersegurança 2019: Cybersecurity Act

2.1. Razões para a criação do regulamento

No Discurso do Estado da União de 2017, proferido pelo Presidente da Comissão Jean-Claude Juncker, foi dada a indicação da criação de um pacote de medidas de cibersegurança como forma de equipar a UE contra as novas inseguranças. O número, a complexidade e a escala de incidentes de cibersegurança tem aumentado e também o seu impacto na economia e na sociedade. Foram descritas várias razões no documento final para justificar a criação de um esquema europeu de certificação de cibersegurança. Uma delas foi o número de dispositivos conectados a aumentar[18] sendo necessário um esforço comum europeu e entre EM para enfrentar as ciberameaças e ter um espaço europeu ciber resiliente. O aumento de cibercrime resultou na criação de iniciativas nacionais arriscando a fragmentar o mercado e criar barreiras de interoperabilidade (por exemplo há três certificações diferentes para *smart meter*, RU, FR, GER). As fragmentações de esquemas de certificação não serão resolvidas sem uma intervenção, à medida que iam surgindo novas vulnerabilidades eram criadas novas certificações a nível nacional. A certificação elaborada de forma transparente ao harmonizar procedimentos e com um conjunto claro de regras para criar esquemas de certificação europeus ultrapassa a fragmentação e cria certificados mutuamente reconhecidos pela União. Os ciberataques comprometeram a confiança dos consumidores e empresas no mercado único, tornasse necessário reforçar a confiança de uma maneira informativa e transparente dos produtos, processos e serviços TIC[19]. A escolha de utilizar certificação vem de uma necessidade de regular ferramentas que já existem no mercado, mas também utilizar a experiência desses instrumentos e canalizar para objetivos específicos europeus (Kamara 2020).

A maioria das razões dadas para estabelecer o esquema de certificação europeu são focadas em incentivar empresas de voluntariamente aumentarem a sua cibersegurança e o comércio de produtos e serviços, em que os consumidores vão beneficiar de maior cibersegurança de forma indireta (Veldhoen 2019). Outro autor (Sivan-Sevilla 2020) é da mesma opinião de que a certificação é teoricamente um caso de integração de mercado para produtos certificados, em que se dá a integração de poderes estatais ao mobilizar capacidades de estabelecer standards e

[18] Cybersecurity Act, Cláusula 2
[19] Cybersecurity Act, Cláusula 7

certifica as infraestruturas sensíveis nacionais. A integração apresenta dois tipos de integração diferentes, uma supranacional e outra intergovernamental, pelo que a presença destes dois métodos revela a dificuldade de elaborar uma política de integração de mercado para assuntos em que toca em poderes estatais.

Em dezembro de 2018 a Comissão, Parlamento e Conselho chegaram a um entendimento no Regulamento e a março de 2019 foi adotado pelo Parlamento, o Conselho aprovou em abril de 2019, culminando na assinatura e aprovação do Regulamento de Cibersegurança no próprio mês.

O Regulamento Cibersegurança (UE 2019/881), contém seis capítulos e 69 artigos, dividido em três partes. No Título I encontram-se as disposições gerais onde se descreve o objetivo do regulamento, que tem em vista assegurar o bom funcionamento do mercado, aumentar a cibersegurança, a ciber resiliência e a confiança na União. Estabelece o âmbito de aplicação do regulamento que são a mudança de objetivos e atribuições de ENISA e a criação de um sistema europeu de certificação "com o objetivo de assegurar um nível adequado de cibersegurança (…) e de evitar a fragmentação do mercado interno no que toca aos sistemas de certificação"[20]. Segundo Bendiek e Schallbruch (2019) a escolha de certificação é baseado na ideia de que padrões e normas criam um balanço entre proteção do consumidor e a necessidade de manter a indústria competitiva, sem estar restrita a vários requisitos.

2.2. ENISA e GECC

O Título II é dedicado às mudanças na ENISA, descrição dos objetivos e atribuições da agência. Ao incluir ENISA no regulamento de cibersegurança é demonstrado a necessidade da Comissão em querer que este regulamento seja aprovado, por ENISA ser um órgão importante (Sivan-Sevilla 2020). A ENISA tem o objetivo de alcançar um nível alto comum de cibersegurança na UE, atuando como um ponto de referência em matéria de aconselhamento com conhecimento especializado em cibersegurança, apoiando assim os EM, instituições, órgãos e organismos europeus. A ENISA tem como nova capacidade de promoção e apoio na elaboração e execução da política europeia de certificação de cibersegurança. Acompanha a evolução na normalização e especificidades técnicas, elabora projetos de esquemas, avalia os sistemas europeus de certificação, presta assistência à comissão e analisa regularmente as tendências do mercado em relação a cibersegurança. A agência informa o público sobre as tecnologias emergentes e avalia o seu impacto na sociedade e economia, realiza análises estratégicas de novas ciberameaças

[20] Cybersecurity Act, artigo 1.º

para prevenir incidentes, presta aconselhamento e disponibiliza orientações para cibersegurança dos cidadãos, organizações e empresas em toda a UE.

Outra novidade neste regulamento é a criação do GECC o Grupo Europeu para a Certificação de Cibersegurança[21], que é composto por representantes das autoridades nacionais de certificação, também podem ser convidados terceiros relevantes. A comissão preside ao GECC e assegura a prestação de serviços com a assistência da ENISA. O GECC tem o encargo de aconselhar e assistir a Comissão ao assegurar a aplicação coerente deste regulamento, do programa de trabalho evolutivo (URWP) da UE e a elaboração de sistemas europeus de certificação, aconselhar e cooperar com ENISA. Pode iniciar um esquema de certificação ao solicitar à Comissão para iniciar o processo e para ENISA elaborar projetos de sistemas de certificação. No seguimento do mesmo, ENISA prepara a proposta de esquema tendo em conta a opinião de vários intervenientes (GECC, Stakeholder Cybersecurity Certification Group SCCG, *working groups* internos, organismos de acreditação nacional, órgãos de estandardização, empresas públicas e privadas). A proposta é entregue à Comissão que pode adotar através de um ato de execução[22], o esquema de certificação é mantido e revisto de cinco em cinco anos (ver figura 1). Se o esquema proposto não for aceitável, a Comissão e o GECC podem pedir a ENISA que prepare outro esquema candidato ou que reveja esquemas existentes não incluídos no programa (URWP). O GECC também dá opinião em relação à manutenção e revisão dos sistemas de certificação, facilita a cooperação entre as autoridades nacionais, reforça o intercâmbio de informação e alinha os sistemas europeus de certificação de cibersegurança com as normas reconhecidas a nível internacional. Com o GECC as autoridades nacionais têm a possibilidade de vetar esquemas de certificação se for assunto de segurança nacional e, portanto, apenas de soberania nacional (Sivan-Sevilla 2020). Os argumentos dados para defesa de cibersegurança como parte de soberania nacional são de que como é um componente das infraestruturas criticas e de proteção de ativos nacionais, continua a ser de responsabilidade nacional dentro dos tratados europeus, em que os EM sentem a necessidade de impor o seu mandato sobre os outros atores e uma falta de confiança de atores externos, não só a UE mas também outros órgãos nacionais, como por exemplo agencias de acreditação nacionais (Sivan-Sevilla 2020).

[21] Cybersecurity Act, artigo 62.º
[22] Tratado sobre o funcionamento da União Europeia artigo 291.º

2.3. Certificação

A parte sobre a certificação no regulamento de cibersegurança começa no Título III sobre o enquadramento para a certificação de cibersegurança. Até ao presente regulamento a certificação era emitida de quatro formas diferentes: a nível internacional, europeu, nacional e indústria. Em primeiro lugar, a nível internacional os certificados são baseados no standard *Common Criteria* (CC). Com o Commom Criteria Recognition Agreement (CCRA) os assinantes aceitam as avaliações feitas pelos seus membros. Enquanto os standards são acordos internacionais, os Estados controlam o processo de acreditação e certificação por agências de defesa nacional e ciber. Em segundo lugar, a nível europeu estabelecido em 1997 com o acordo de mútuo reconhecimento entre doze EM e Noruega sobre certificação CC, conhecido como o Acordo de Seniors Officials Group on Information System Securty (SOG-IS). Os propósitos da criação do SOG-IS são de coordenar a estandardização de CC, coordenar as políticas de certificação entre os órgãos públicos dos EM e coordenar o desenvolvimento de esquemas de certificação que cumpram os requisitos legais a nível europeu. O alcance do acordo é limitado a produtos que envolvam assinaturas digitais, tacógrafo digital[23] e *smart cards*. As autoridades nacionais quiseram limitar os níveis altos de standard CC a domínios técnicos específicos onde acordos dos métodos de avaliação e requisitos já existiam (Sivan-Sevilla 2020). Os EM concordam em standard, controlam a acreditação, certificação e práticas de avaliação. Em terceiro lugar, a nível nacional nos quais os órgãos públicos de certificação estabelecem certificados reconhecidos apenas dentro do próprio país. Não são todos os EM que têm capacidades de certificação e conhecimento, isto cria diferente posições de partida para a aplicação do esquema europeu de certificação. Por último, a nível da indústria em que o privado escolhe os standard, acreditação, certificação e avaliação. Associações industriais adotam standard e emitem certificados reconhecidos dentro de setores industriais.

Com o Cybersecurity Act, foram criadas três opções de certificação que são básico, substancial e elevado, os requisitos de segurança que corresponde a cada nível são fornecidos no sistema europeu de certificação[24]. Uma harmonização uniforme para todos os produtos é impossível de desenvolver devido à variedade de produtos e certificados existentes, por isso no regulamento dividem em níveis de garantia que são proporcionais ao nível de risco associado à utilização prevista do produto. No nível básico os produtores/fabricante ou prestador de serviços podem renovar o certificado com uma autoavaliação da conformidade, apresentando

[23] Dispositivos instalado em carros que regista a velocidade, distância e atividade do motorista
[24] Cybersecurity Act, artigo 52.º

uma cópia à autoridade nacional de certificação e a ENISA, que demonstre o cumprimento dos requisitos estabelecidos no sistema. A declaração de conformidade não é um certificado, o produtor assume a responsabilidade de seguir o regulamento, enquanto que um certificado envolve avaliação de terceiros (Kamara 2020). No nível substancial pode ser feito pelo público ou privado, o que permite ao privado trabalhar com atores de mercado de vários países e produzir certificados reconhecidos na UE. A avaliação é realizada em laboratórios privados, acreditação é um esforço conjunto por órgãos nacionais e de acreditação (Sivan-Sevilla 2020). No nível de garantia elevado o certificado só pode ser emitido por uma autoridade nacional de certificação. "A certificação é voluntária, salvo disposição contrário no direito da União ou dos Estados-Membros."[25], portanto não há qualquer obrigação ou incentivo para a certificação. Segundo Mitrakas (2018) a certificação voluntária é uma forma de harmonizar a lei de cibersegurança através do esquema de certificação europeu, que contêm esquemas específicos para produtos específicos com requisitos mínimos de segurança que são aprovados por todos os EM. A Comissão avalia a necessidade de alguns sistemas serem de certificação obrigatória para alguns produtos que não tenham um nível adequado de certificação, o nível de segurança depende do risco percecionado que é com base no uso e importância, nesse caso a comissão dá prioridade às infraestruturas críticas (Voldhoen 2019). A primeira avaliação dos sistemas de certificação deve ser realizada ate 31 de dezembro de 2023 e posteriormente de dois em dois anos.

A Comissão publica o programa de trabalho evolutivo (URWP) para a certificação europeia, no qual compreende uma lista dos produtos, serviços e processos TIC que podem beneficiar, em termos de cibersegurança, ao serem incluídos no esquema de certificação e é atualizado de três em três anos[26]. O programa já foi publicado e tem como linhas de ação: melhorar o desenvolvimento e implementação de standard, gestão de risco, promover segurança desde o início, configurar de forma segura como padrão, consistência entre esquemas, cooperação internacional para saber os standards e métodos existentes. Os esquemas identificados como prioritários são 5G por envolver infraestruturas críticas e em conjunto com o 5G toolbox, componentes industriais de infraestruturas críticas, internet das coisas com diferentes níveis de segurança, inteligência artificial, criptografia e ciclo de vida de seguros.

[25] Cybersecurity Act, artigo 53.º e 56.º
[26] Cybersecurity Act, artigo 47.º

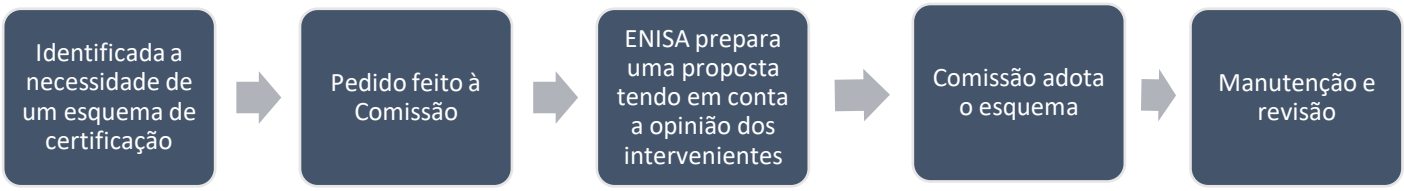

Figura 1. Processo criação de um esquema certificação, com base no artigo Mitrakas (2018)

2.4. Autoridade Nacional

Uma mudança importante com o regulamento são as alterações às autoridades nacionais de certificação[27]. Os Estados não podem produzir novos sistemas nacionais de certificação, mas os certificados emitidos por essas autoridades continuam válidos até caducarem. Os produtos, serviços e/ou processos que não sejam abrangidos pela certificação continuam a existir, mas os que interferem deixam de produzir efeito, caso haja a intenção dos estados de elaborarem um novo sistema de certificação de cibersegurança devem comunicar à Comissão e ao GECC. Todos os estados membros necessitam de uma autoridade nacional de certificação dentro do seu território ou uma autoridade nacional de certificação estabelecida noutro Estado, com o acordo desse Estado[28]. A nível operacional compete às autoridades nacionais a supervisão e aplicação das regras do presente regulamento em cooperação com outras autoridades de fiscalização do mercado, controlar o cumprimento das obrigações de fabricantes, prestadores de serviços e fornecedores, autoavaliação, tratar as reclamações apresentadas e investigar o objetos das reclamações informando os autores da mesma do andamento e do resultado da investigação. Para além disso, fornecer a ENISA e ao GECC um relatório anual de síntese das atividades realizadas, cooperar com outras autoridades nacionais e públicas de cibersegurança na partilha de informação de conformidade com a certificação, acompanhar factos relevantes na certificação de cibersegurança, conduzir auditorias aos organismos de avaliação de conformidade e aos titulares de certificados, retirar o certificado às que não cumprem o regulamento, aplicação de sanções de acordo com o direito nacional e exigir a cessação da violação. As autoridades nacionais acreditam os organismos de conformidade, essa acreditação tem um prazo de cinco anos.

Com o novo regulamento, os esquemas de certificação europeu são produzidos pela primeira vez num processo facilitado pelas instituições europeias, mas sob o controlo das

[27] Cybersecurity Act, artigo 57.º e 58.º
[28] Cybersecurity Act, artigo 58.º

autoridades nacionais. A acreditação é reconhecida por todos os EM e opera de maneira intergovernamental com o mecanismo de analise pelos pares[29]. As autoridades nacionais de certificação de cibersegurança são sujeitas a análise pelos pares realizada com base em critérios e procedimentos transparentes de avaliação. A análise de pares é realizada por outras autoridades nacionais de certificação de cibersegurança e pela comissão, no mínimo uma vez em cada cinco anos, os resultados da análise dos pares são examinados pelo GECC. Este mecanismo aumenta o controlo das autoridades nacionais sobre os órgãos de certificação privados e assegura standards e práticas equivalentes pela UE prevenindo uma descida da qualidade de certificação (Sivan-Sevilla 2020). As autoridades nacionais querem mais controlo para assegurar a qualidade de certificação, mas o privado foi elevado para aumentar as capacidades europeias em métodos de avaliação de certificação (Sivan-Sevilla 2020).

[29] Cybersecurity Act, artigo 59.º

CAPÍTULO 3

Metodologia

O modelo Advocacy Coalition Framework (ACF) proposto por Paul Sabatier, em 1988, constitui-se como uma alternativa ao modelo heurístico de análise do processo político, uma forma de sintetizar as abordagens *top-down* e *bottom-up* e incorporar informação técnica no processo político. O objetivo do modelo é disponibilizar uma ferramenta para compreender as mudanças políticas em setores transversais e multifuncionais. Desde que foi definida em 1988 o modelo sofreu várias revisões (Sabatier, 1988, 1998; 1999; 2007; Sabatier e Jenkins-Smith, 1993; Sabatier e Mcqueen, 2009).

Sabatier (1998) refere que o ACF pode ser aplicado na UE devido às complexas relações existentes e pela maneira de como as instituições nacionais são o principal ponto de mudança política. Na UE existe complexidade temática pela facilidade de comunicação entre atores e uma grande quantidade de informação disponível. O ACF já foi aplicado em várias investigações sobre políticas europeias, na sua maioria em matéria ambiental, indústria e crise energética, Peterson 1995, Richardson 1995 e 1996, Josselin 1996, Coen 1997, Villamor 2006, Weible et al 2016.

Neste trabalho vamos utilizar a variante Sabatier e Mazmanian (1983) modelo de implementação política, para perceber o que realmente acontece a uma política depois de ser formulado, sendo esse o objeto de estudo da implementação de políticas públicas. Este método tem em conta o comportamento dos órgãos administrativos, a rede de influências diretas e indiretas e as características da sociedade. Ademais, reconhecendo os fatores sociais, institucionais e económicos imutáveis perante a estruturação da política pública. Também igual ao modelo de coligações em que interpreta os contributos dos órgãos e atores em coligações, onde as coligações competem entre si e o poder é determinado pela sua habilidade em implementar vontades e interesses com os recursos que possuem.

Anteriormente ao estudo da implementação, se os objetivos não estivessem a ser atingidos, a solução seria criar sistemas administrativos mais racionais, científicos, eficientes e hierarquicamente estruturados. Eram apenas considerados os problemas na parte legislativa da criação da política sem ser considerado a sua execução. Para Sabatier e Mazmanian (1983) as agências administrativas não só são afetadas por mandatos legais, mas também por pressão de grupos de interesse. Também foram identificados limites ao controlo por hierarquia (limites em

termos de cognição racional, comunicação distorcida e dificuldade de monitorizar comportamentos) e com o uso da teoria de uma abordagem sistemática à vida política, que permite pensar em fatores fora da área administrativa como diretivas legislativas diferentes, mudanças na opinião pública e novas tecnologias. Foi a perceção de falha e falta de conformidade que deu aso à investigação de relações entre política públicas e os resultados da implementação da administração.

Há distinções claras entre formulação/ adoção de políticas, implementação e reformulação pelos políticos que criaram, com base no sucesso e dificuldades de implementação, há uma separação de legislação e agências administrativas como executores. Todos os estudos de implementação procuram avaliar o programa, também podem ser distinguidos pelo foco em resultados ou possíveis resultados. Neste trabalho vamos analisar os possíveis resultados, por esta política ter entrado em funcionamento apenas em 2019 e por isso não haver dados de resultados ou avaliações.

Segundo Sabatier e Mazmanian (1983) a implementação pode ser vista de três perspetivas diferentes: legislador, implementadores e grupo alvo. A implementação envolve obter conformidade do grupo alvo para mudar comportamentos. Os legisladores preocupam-se quais medidas foram cumpridas e razões para não serem, os implementadores focam-se como as instituições respondem às mudanças causadas pela nova política e na perspetiva do grupo alvo se a nova política faz alguma diferença na vida deles, podem se focar nas dificuldades de seguir o regulamento.

CAPÍTULO 4

Análise: implementação do regulamento de cibersegurança

A metodologia de análise que vamos utilizar é a variante Sabatier e Mazmanian (1983) modelo de implementação política. O objetivo desta pesquisa é analisar os diferentes processos de interação que culminaram no Regulamento de Cibersegurança (2019) e se com a implementação vai conseguir harmonizar os esquemas de certificação de cibersegurança na europa, aumentar a confiança no mercado e a cibersegurança dos produtos e serviços.

A temática de investigação é certificação de cibersegurança por isso o subsistema que vou analisar é o de cibersegurança. O ciber ecossistema é complexo e multifacetado, dentro de várias áreas de políticas internas com a justiça, assuntos internos, o mercado único digital, cibersegurança na diplomacia e política de ciber defesa emergente. Na análise de política de implementação são identificadas variáveis que vão afetar a realização dos objetivos durante o processo. Dividindo em três áreas a sociabilidade dos problemas, a habilidade de estruturar o processo de implementação e redes de variáveis políticas que afetam a implementação, sendo um balanço de suporte entre contra ou a favor dos objetivos estabelecidos.

4.1. Sociabilidade dos problemas

Os aspetos específicos de problemas sociais que afetam a habilidade governamental das instituições de realizar o propósito estabelecido. Mazmanian e Sabatier (1983) separam esta secção em quatro partes, ver figura 2. Para concretizar os objetivos do programa são necessários vários pré-requisitos técnicos e entendimento das causas que ligam ao problema, de forma a desenvolver medidas efetivas e pouco dispendiosas de resolução. O pré-requisito técnico legal no regulamento de cibersegurança, artigo 114 do Tratado sobre o Funcionamento da União Europeia (TFUE), uma aproximação legislativa dos EM para realizar o objetivo de um bom funcionamento do mercado[30] e segundo o princípio de subsidiariedade e proporcionalidade[31] fica ao encargo dos EM a implementação e execução. Foram identificados como problemas a fragmentação de certificação entre EM, recursos dispersos e falta de sensibilização para cibersegurança (Commission Staff Working Document 2017). As diferentes abordagens a standards e certificados de cibersegurança tornam difícil criar requisitos mínimos de segurança

[30] Tratado sobre o Funcionamento da União Europeia (TFUE) artigo 26.º
[31] Tratado da União Europeia (TUE) artigo 5.º

no mercado europeu. A falta de informação sobre a segurança do produto transmite pouca confiança no mercado comum, diminui a escolha do consumidor, como não conseguem selecionar com base na segurança vão pela reputação do vendedor ou pelo preço, isto orienta para uma corrida ao último lugar em investimentos e recursos de segurança. Também diminui a competitividade de empresas europeias e dependência de produtos e serviços fora da União.

As dificuldades técnicas em cibersegurança são devido a ser uma área em desenvolvimento, portanto para novos produtos não existem ainda standards e requisitos de segurança, e não podem ser muito restritos senão limitam a inovação. Ademais, a cibersegurança envolve vários dispositivos diferentes em diversas áreas por isso não há um esquema universal, tem de ser feito à medida e atualizado ao longo do tempo.

É preciso reconhecer o comportamento do grupo alvo a ser regulamentado, de forma a compor regras que moderem o comportando para obter a conclusão desejada, devido às diferenças do seu compromisso com o regulamento pode resultar em variações, especialmente neste regulamento que é de adesão voluntária. Na UE aplicam um critério de avaliação de sistemas de segurança o SOG-IS, reconhece certificados europeus com o Mutual Recognition Agreement of Information Technology Security Certificates (SOG-IS MRA), que aplica o CC. Pertencem à SOG-IS dezassete países, dos quais sete são emissores de certificados, seis dos sete países também são assinantes do CCRA. Com o novo esquema candidato (2020)[32] vai se passar a utilizar EU-CC como sucessor dos esquemas de certificação existentes SOG-IS MRA. O mercado único é fragmentado devido à existência de vários certificados nacionais, por exemplo o esquema de certificação francês desenvolvido pelo ANSSI e o esquema alemão desenvolvido pelo BSI não se reconhecem um ao outro, o esquema do Reino Unido é apenas reconhecido dentro do mesmo, também não é permitido a venda de serviços sem os ter certificado. No mercado italiano não é obrigatório certificar, mas é necessário seguir os requisitos e os padrões estabelecidos para infraestruturas críticas como comunicação, finanças, energia, transportes e saúde é sempre necessária certificação, em França é necessária autorização do gabinete do primeiro-ministro, o que torna todo o processo lento e custoso.

O grupo alvo da política são todos os afetados por problemas de cibersegurança – empresas, autoridades públicas e cidadãos. Os produtores e vendedores sofrem com falta de recurso e existências de múltiplos esquemas de certificação, os compradores de produtos TIC para indústria são afetados pela falta de informação das propriedades de segurança do produto. As

[32] EU cybersecurity certification framework: draft candidate EU-CC certification scheme, Andreas Mitrakas in European Accreditation Conference, 26/11/2020

autoridades públicas sofrem de insuficiente suporte técnico para estabelecer melhores práticas e implementar políticas europeias. Os cidadãos pouco sensibilizados para ciberameaças são expostos a riscos, tendo de suportar os custos de reparação e fuga de informação pessoal, e por não terem conhecimento da segurança nos produtos e serviços a circular no mercado.

É necessário um certo grau de mudança no comportamento dos intervenientes para a política ser implementada corretamente, quanto maior for a mudança em comportamento mais difícil é de se atingir os objetivos. No preâmbulo do regulamento de cibersegurança é identificado uma necessidade geral de sensibilização dos cidadãos, organizações e empresas para questões de cibersegurança, divulgação de vulnerabilidades entre empresas, organizações, órgãos e consumidores. Também necessária uma transição para a nova certificação europeia de forma harmoniosa e homogénea em todos os EM, deixando de criar esquemas nacionais de certificação, adotando o sistema europeu de certificação de cibersegurança na legislação nacional e designar uma autoridade nacional de certificação de cibersegurança para supervisionar o cumprimento do regulamento. Os fabricantes devem atualizar os seus produtos para as novas normas europeias de segurança, os importadores e distribuidores devem assegurar que os produtos inseridos no mercado cumprem os requisitos de segurança. A escolha de certificação e dos requisitos de segurança deve basear-se numa análise dos riscos associados à utilização do produto, serviços ou processo TIC.

4.2. Habilidade de estruturar o processo de implementação

Um regulamento, diretiva ou ordem governamental estrutura o processo de implementação pela delineação de objetivos legais e pela escolha de organizações de implementação, ao facultar recursos legais e financeiros com orientações politicais aos oficiais das agências e ao regular oportunidades de participantes não governamentais de aderirem ao processo de implementação. Os objetivos legais precisos e claros são uma ajuda indispensável na avaliação de um programa e mais provável de os resultados serem os esperados das agências de implementação e do comportamento do grupo alvo. Quando uma nova política é dada a uma organização já existente é necessário indicar a prioridade em relação ao programa existente do órgão. Os objetivos do Regulamento de Cibersegurança são de assegurar o bom funcionamento do mercado interno, aumentar o nível de cibersegurança, resiliência e confiança dentro da União[33]. Nos objetivos de ENISA são enumerados sete[34]: centro de conhecimento especializado em matéria de

[33] Cybersecurity Act artigo. º1
[34] Cybersecurity Act artigo. º4

cibersegurança; prestar assistência às instituições, órgãos e organismos da UE e EM sobre políticas de cibersegurança europeia; apoiar o reforço de capacidades de cibersegurança e resiliência da UE e dos EM; promover a cooperação e a partilha de informação entre UE, EM, partes interessadas do setor publico e privado; ajudar os EM na prevenção e resposta a ciberameaças; promover o recurso a certificação europeia de cibersegurança, contribuindo para a sua criação e manutenção; promover sensibilização em matéria de cibersegurança, ciber higiene e literacia digital dos cidadãos, organizações e empresas. O esquema de certificação de cibersegurança está em penúltimo na lista de prioridades da ENISA, segundo Sabatier e Mazmanian (1983) pode resultar na política ser atrasada devido a baixa prioridade, em comparação com as outras operações.

Todas as políticas contêm uma teoria causal na qual são especificados de como os seus objetivos devem ser atingidos. Uma teoria causal requer um elo causal entre a intervenção do governo e os objetivos do programa para ser percebido e que os oficiais executivos responsáveis pela implementação tenham jurisdição suficiente para atingir os objetivos. O fornecimento de produtos de cibersegurança no mercado europeu é fragmentado, por a indústria na UE se ter desenvolvido consoante a necessidade nacional e o uso de produtos importados. A certificação de cibersegurança também é fragmentada e utilizada de forma limitada a nível dos EM, com os seus próprios requisitos técnicos, metodologias de ensaio e procedimentos de certificação de cibersegurança, portanto é necessário adotar uma abordagem comum europeia de certificação. A certificação de cibersegurança vai ajudar a aumentar a confiança nos produtos, serviços e processos de TIC, evitando a multiplicidade de sistemas nacionais e aumentando a resiliência de cibersegurança da União. A cibersegurança é uma questão de interesse comum da União, em que já há de tal ordem uma interdependência de redes que os EM individualmente são incapazes de enfrentar ameaças, gerir riscos e impactos de ciber incidentes.

Os recursos financeiros são necessários para concretizar as novas atribuições da Diretiva NIS e quadro europeu de certificação de cibersegurança, para contratar recursos humanos, pessoal especializado de análise técnica, monitorização e outros serviços necessários. Os documentos públicos disponíveis não especificam o orçamento dado ao regulamento, mas inclui um aumento nos recursos financeiros de ENISA. No documento de proposta da política apresentem uma estimativa de 10,739 milhões e 16,550 milhões pedido para 2019, para 2020 previsto 10,954 milhões e 20,646 milhões pedidos, de 2021 para a frente é uma estimativa porque quando foi desenvolvida a proposta de regulamento ainda não havia orçamento 2021-2027. Para 2021 foi pedido 22,248 milhões e para 2022 foi pedido 23,023 milhões, segundo o programa de trabalho de ENISA 2021-2023 é esperado um aumento gradual do orçamento.

Um dos atributos mais importantes de qualquer política pública é a extensão de integração hierárquica dos órgãos de implementação, dependendo de como o sistema está integrado e do grau de concordância entre oficiais das medidas para executar. Resistência a medidas ou recomendações voluntárias pode ser resolvido com sanções ou incentivos para modificar comportamentos. No caso do Regulamento de Cibersegurança tem indicações de mudanças e implementação para os Estados e empresas executarem de forma voluntária. A nível nacional cada EM nomeia uma autoridade nacional de certificação de cibersegurança que compete supervisionar e aplicar as regras do regulamento, em cooperação com outras autoridades de fiscalização do mercado. O GECC é composto por representantes das autoridades nacionais, o qual assiste ENISA na elaboração de propostas de sistemas, adota pareceres à comissão em relação à manutenção e revisão de alguns sistemas europeus de certificação de cibersegurança. Também facilita a cooperação entre autoridades nacionais reforçando capacidades e intercâmbio de informação, facilita o alinhamento do sistema europeu com as normas internacionais formulando recomendações. Portanto a Comissão adota esquemas proposto por ENISA com pareceres de GECC e as autoridades nacionais com o apoio de ENISA e coordenação de GECC implementam a nível nacional.

Uma política pública pode influenciar o processo de implementação ao estipular regras formais de decisão das agências de implementação. Como um produto para ter um certificado europeu de cibersegurança precisa de seguir os elementos estipulados no regulamento (art.º 51, 52, 54 e 56) as empresas necessitam de disponibilizar toda a informação necessária sobre vulnerabilidades, irregularidades e cumprir os requisitos para obter a certificação das autoridades nacionais de certificação, aplicando assim o regulamento.

4.3. Redes de variáveis políticas que afetam a implementação

Enquanto um regulamento estabelece a estrutura legal em como vai ser executada, a implementação tem um dinamismo conduzido por dois processos: a necessidade de receber suporte político de forma constante para o processo de adoção não ser arrastado e esquecido e as mudanças socioeconómicas e tecnológicas que suportam os objetivos da política. Segundo Sabatier e Mazmanian (1983) os resultados de implementação são uma função da interação entre a estrutura legal e o processo político, visto que a implementação fica dependente das variações do suporte político ao longo do tempo e a nível local. Nesta secção, terceira caixa na figura 2, vamos falar das variáveis externas: mudanças nas condições socioeconómicas, suporte

do público/população, atitudes do soberano e do grupo eleitorado, e a habilidade de liderança dos responsáveis por implementação.

A variação de condições socioeconómicas ao longo do tempo dificultam a acessibilidade dos objetivos pretendidos, podem afetar a perceção da importância do problema, dando prioridade a outros problemas transitando também os recursos disponíveis. Com uma grande variação das condições socioeconómicas locais torna-se difícil implementar com êxito, havendo uma mudança de foco da problemática e pressão para medidas mais flexíveis. No mesmo ano em que o regulamento entra em efeito, 2019, é quando a comissão de Ursula von der Leyen começou, dezembro 2019-2024, com a proposta de Green Deal e inovação digital, inclui cibersegurança, educação digital, inteligência artificial, supercomputação e 5G. Quando a pandemia atingiu a europa em 2020 pós em prova os sistemas nacionais de saúde e a economia europeia, as restrições impostas para conter a propagação do vírus abrandaram a vida económica, perturbando as cadeias de abastecimento, produção e interrompeu o comércio de bens e serviços. Como resposta a UE lançou um plano de recuperação chamado Next Generation EU investindo em três pilares: apoio aos EM destinado ao investimento e reformas para fazer face à crise, revitalizar a economia europeia ao criar incentivos ao investimento privado, aprender com a crise ao criar um programa europeu para a saúde para preparar para futuras situações de crise. O plano Next Generation EU também promove as propostas iniciais de crescimento ecológico e inovação digital.

A variação do apoio público ao longo do tempo de objetivos políticos é uma variável que afeta a implementação. Segundo Down (1972) a atenção pública segue um ciclo que começa com um acordar inicial para o problema seguido de um declínio quando se percebe os custos necessários para a sua resolução e o surgimento de outros assuntos na agenda política ou escândalos. Contudo o apoio pode ser reacendido com novas evidências de que o problema persiste (exemplo no caso em específico, vários ciberataques). O público pode influenciar o método de implementação de três maneiras: ao dar a sua opinião interagindo com os media, influências dos constituintes (em assuntos locais) e em consultas públicas. Antes de o Regulamento de Cibersegurança ser proposto pela comissão houve várias consultas públicas sobre ENISA, roadmap[35] do esquema de certificação europeu e uma segunda consulta depois

[35] Na UE utiliza vários tipos de consulta pública com determinados objetivos, no roadmaps a formulação de novas ideias políticas e legislativas, os cidadãos podem dar a sua opinião no prazo de quatro semanas. A proposta legislativa, depois de a comissão finalizar a proposta legislativa e submetê-la ao parlamento e ao conselho para decidirem abre um novo período de consultação com o prazo de oito semanas, no qual as contribuições dadas serão passadas aos órgãos decisores.

da comissão propor o regulamento, também houve workshops desenvolvidos por ENISA sobre certificação.

A consulta pública realizada de 18 de janeiro a 12 de abril de 2017 sobre a avaliação do desenvolvimento de ENISA durante o mandato de 2013-2016. Na primeira questão, de quais serão as maiores necessidades nos próximos 10 anos no setor de cibersegurança, 48 responderam cooperação entre os estados-membros, 44 a capacidade de prevenir, detetar e resolver ataques cibernéticos de grande escala. Também perguntaram aos participantes as áreas em que ENISA podia ter impacto e as áreas em que não teria, nas que não teria identificaram harmonização de standards e a certificação de produtos TIC e serviços. Os participantes veem ENISA como um órgão para fomentar cooperação entre organismos e estados, sendo essa opção que obteve mais respostas. Entre os participantes dos 84 que responderam à segunda parte, apenas 23 votaram a favor da certificação. A consulta pública realizada de 7 de julho a 4 de agosto do roadmap para receber a opinião em relação a certificação de cibersegurança a nível europeu, a maioria votou numa certificação com base no New Legislative Framework de 2008[36], sendo os catorze participantes todos empresas de várias dimensões. Na consulta pública de setembro a dezembro de 2017 para comentar sobre a proposta de regulamento de cibersegurança e esquema de certificação de cibersegurança europeu, houve 32 respostas. Os participantes na sua maioria são empresas, no qual todos os participantes concordaram com a reforma de ENISA e de ter um mandato permanente. Sobre certificação 30 pessoas comentaram com 73% em favor de um esquema europeu de cibersegurança. PME em resposta a um questionário sobre existência de várias certificações em TIC disseram que representa uma barreira para a entrada no mercado por ter elevados custos, da mesma opinião na consulta pública de cPPP (dezembro 2015 a março 2016) de que é uma barreira para a entrada no mercado devido a custos de conformidade com as várias certificações e deve ser evitado uma maior fragmentação. Nos anexos encontrasse por extenso os dados encontrados nas várias consultas públicas.

Mudanças no recurso e atitudes dos grupos apoiantes dos objetivos constitui uma parte importante do processo de implementação. A tarefa essencial é traduzir o apoio inicial que ajudou a passar a legislação para organizações com membros, experiência e coesão para serem aceites como legítimas podendo implementar e sugerir mudanças políticas. Os grupos apoiantes

[36] Regulamento (EC) No 765/2008, que estabelece os requisitos de acreditação e fiscalização do mercado relativos à comercialização de produtos, dentro da europa e vindo de países terceiros. Para garantir que os produtos cumprem os requisitos e que asseguram um elevado nível de proteção do interesse público em domínios como a saúde e a segurança em geral, a saúde e segurança no local de trabalho, a defesa do consumidor, a proteção do ambiente e a segurança.

podem intervir na implementação ao comentar nas decisões propostas e ao disponibilizar recursos. Várias empresas de diversas áreas intervieram e deram a sua opinião nas várias consultas públicas. Devido ao grande interesse e elevado valor da opinião do privado para implementar uma certificação de cibersegurança europeia foi criado o SCCG, teve a sua primeira reunião a 24 junho de 2020 e tem como membros órgãos europeus de standard, empresas de várias áreas e academia. Este grupo tem como objetivo aconselhar ENISA sobre as propostas de esquemas de certificação.

Os soberanos das instituições encarregues da execução proporcionam apoio aos objetivos através de supervisão direcionada, recursos financeiros e extensão de mandatos. No caso do Regulamento de Cibersegurança, a Comissão estendeu o mandado de ENISA e implementa os esquemas de certificação de cibersegurança a nível europeu por um ato de implementação. A nível local quem supervisiona os esquemas de certificação e a sua aplicação são as autoridades nacionais de certificação. Segundo o regulamento os EM têm ate junho de 2021 para criarem ou nomearam a sua autoridade nacional de certificação. Os participantes no SOG-IS já tem uma autoridade nacional de cibersegurança a priori. Segundo Sivan-Sevilla (2020) os EM dominaram o processo de integração e negociação da proposta e como resultados escolheram um regime parecido com o anterior, em que tem controlo nacional com o GECC. Portanto como estiveram envolvidos no processo da sua criação à partida estão de acordo.

Segundo Sabatier e Mazmanian (1983) o compromisso dos oficiais que vão realizar os objetivos é a variável que afeta mais diretamente os resultados do processo de implementação. Pode ser caracterizada de duas formas, a hierarquia dos objetivos nas prioridades de execução e a habilidade de realizar essas prioridades. No caso do regulamento quem implementa a nível nacional são as autoridades nacionais de certificação, as prioridades e habilidades que cada uma das autoridades nacionais de certificação possui é algo a ser analisado caso a caso.

4.4. O processo de implementação por fases

A análise tem se focado até agora nos fatores que afetam a implementação no geral, mas esse processo também é visto por fases: rendimento das políticas (decisões) das agências de implementação, a adesão do grupo alvo às decisões tomadas, o impacto real das decisões da agência, os impactos percecionados e por fim a avaliação da política pública e se são necessárias revisões. Cada um destas fases pode ser pensado como uma variável dependente e também afeta a fase seguinte.

Os objetivos do regulamento devem ser traduzidos em medidas operacionais capazes de serem aplicadas concretamente e este processo requer esforço por partes dos oficiais que vão executar a nível local para analisar de forma técnica de como aplicar as regras em situações concretas e executar essas regras em casos específicos. Algumas discrepâncias entre objetivos e decisões políticas tomadas pelos oficias são inevitáveis, essas diferenças podem ser reduzidas com objetivos claros. Ainda mais, os objetivos foram referidos anteriormente de assegurar o bom funcionamento do mercado interno, aumentar o nível de cibersegurança, resiliência e confiança dentro da UE. Além disso, o impacto esperado é de aumentar a capacidade de preparação dos EM e empresas com o uso de certificação, sendo uma forma de diminuir as vulnerabilidades em infraestruturas, evitar fragmentação de esquemas de certificação, harmonizando os esquemas nacionais existentes e impedindo de criar esquemas que vão se sobrepor aos esquemas de certificação de cibersegurança europeus. ENISA suporta o desenvolvimento e manutenção dos esquemas de certificação de cibersegurança europeus e aumenta a sensibilização dos cidadãos para cibersegurança com a disseminação de boas práticas de ciber higiene.

Segundo Sabatier e Mazmanian (1983) o nível de conformidade do grupo alvo com os objetivos políticos são de acordo com os seguintes fatores: um resultado de a probabilidade de ser detetado o seu não incumprimento e ser castigado com êxito, a existências de sanções para penalizar, as atitudes do grupo alvo consoante a legitimidade do regulamento estabelecido e os custos de atuar em conformidade. De acordo com as consultas públicas a maioria dos intervenientes de áreas diferentes, administração pública, empresas de grande dimensão e PME são de acordo com o regulamento de cibersegurança e de implementar o esquema europeus de certificação de cibersegurança europeu. No entanto, a adesão à certificação de cibersegurança é voluntária, mas por contratação pública pode se tornar obrigatório. As sanções são estabelecidas pelos EM[37] e eles próprios tomam as medidas necessárias para as aplicar. Os custos paras as empresas que já certificavam vai diminuir em custos administrativos e para os que não certificam é sem custos, uma vez que é uma medida voluntária. Contudo o mútuo reconhecimento de esquemas de certificação de cibersegurança vai aumentar a competitividade de empresas transnacionais e diminuir a barreira de mercado, especialmente para as PME que contribuem para uma transição digital rápida.

[37] Cybersecurity Act artigo 65.º

Durante esta análise é importa saber quais os objetivos que foram realizados e consoante Sabatier e Mazmanian (1983) uma política vai conseguir os impactos desejados se os resultados dos agentes de implementação são consistentes com os objetivos do regulamento, se o grupo alvo age de acordo com os objetivos, não há subversão dos objetivos pretendidos e há uma teoria causal que liga a mudança do comportamento do grupo alvo com a realização dos objetivos. Em relação aos objetivos estabelecidos de harmonizar esquemas nacionais existentes, foram submetidas propostas de esquemas de certificação de EUCC e EUCS para serviços Cloud. O EUCS é baseado no standard ISO internacional, nos requisitos de segurança tem como base esquemas nacionais, portanto vai harmonizar os esquemas nacionais francês, alemão e holandês que também têm sobre Cloud. No esquema EUCC é uma transição do SOG-IS com melhorias para manutenção de certificados, atividade harmonizada de monitorização e os certificados vão incluir um rótulo associado ao esquema EUCC, com um QR Code que vai fornecer acesso à informação de certificação. No relatório da consulta pública ao EUCC 64% concorda com a transição de esquema, 82% tem intenção de utilizar o novo certificado e 70% concorda que as melhorias vão ter impacto positivo.

Os impactos de uma política pública podem ser difíceis de medir de uma forma compreensiva e sistemática, é necessário no processo de avaliação do programa ter em conta os impactos percecionados pelo grupo alvo, órgãos responsáveis por implementação e outros interveniente no subsistema. No artigo 67.º sobre avaliação e revisão da ENISA e da certificação de cibersegurança europeia está marcada para junho de 2024, no momento da escrita não está disponível esse documento e não é possível fazer uma análise dos impactos percecionados. Como a fase final de uma política pública é a análise da sua implementação para uma revisão e reformulação do documento, tal também não é possível de momento.

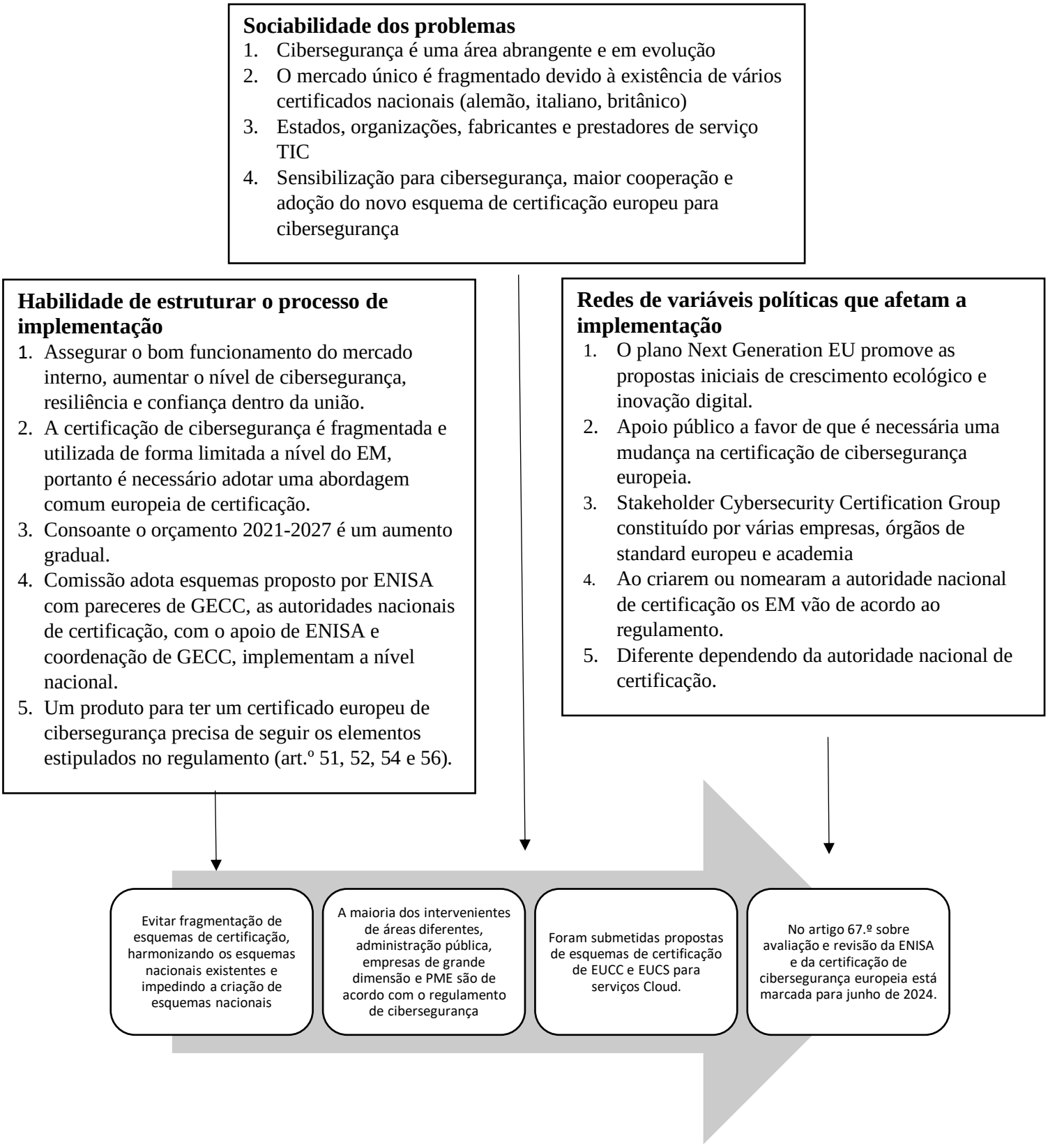

Figura 2. Modelo de implementação política de Sabatier e Mazmanian (1983)

4.5. Estudo de caso – Alemanha

Já vimos como está a acontecer a implementação no geral a nível europeu, com o seguinte modelo vamos analisar um país em específico, como exemplo a Alemanha. Os métodos de implementação deste país podem não ser igual ao dos outros, os EM têm diferentes capacidades de cibersegurança devido aos recursos, experiência e cultura de gestão de risco que impactou o seu nível de preparação. Na área de certificação há países com mais experiência, órgãos de gestão de conformidade criados previamente ao regulamento de cibersegurança, e com diferentes níveis de cooperação público-privado. Segundo Sivan-Sevilla (2020) o interesse dos EM na certificação vêm de que eles já têm capacidades na área e por tocar em assuntos de segurança nacional. A escolha do regime de certificação europeu não é muito diferente do anterior legitimando a posição nacional, como acontece no caso alemão.

O método que vou utilizar para analisar é o modelo do processo de implementação de políticas públicas de Van Meter e Van Horn (1975), o modelo utiliza seis variáveis que influenciam a ligação entre a política pública e o desempenho. Este modelo específica as relações entre variáveis independentes e o desempenho, mas também o relacionamento entre as várias variáveis independentes. Visto que o interesse é identificar fatores que determinem o desempenho de uma política pública é preciso reconhecer indicadores de desempenho, os indicadores de desempenho avaliam em que medida os objetivos da política foram realizados.

Para analisar os objetivos é necessário ir para além das generalidades do documento legislativo para fornecer um modelo concreto e específico para avaliar o desempenho do programa. Tendo em conta o que foi já referido anteriormente, os objetivos do Regulamento de Cibersegurança são de assegurar o bom funcionamento do mercado interno, aumentar o nível de cibersegurança, resiliência e confiança dentro da União. Na comunicação da proposta para o regulamento de cibersegurança (COM 2017 477 final) foram apresentados alguns indicadores de avaliação dos objetivos, que são os seguintes: aumentar o grau de preparação dos EM e empresas; cooperação entre EM e instituições, agências e organismos da UE; aumentar capacidades da UE de complementar a dos EM no caso de cibercrimes; aumento de sensibilidade dos cidadãos e empresas para cibersegurança; reforçar confiança no mercado único digital e uma maior transparência da garantia de cibersegurança.

A segunda variável, a quantidade de recursos disponíveis pela política pública que facilitam a implementação, esses recursos podem incluir fundos ou outros incentivos que possam encorajar. O BSI é a autoridade central de cibersegurança na Alemanha, foi estabelecida por lei federal em 1991 como uma organização de certificação e licenças de sistemas de criptografia para vigilância com propósitos de defesa. A missão do BSI é dividida em três áreas: estabelecer e rever produtos e sistemas de segurança; supervisionar a implementação de medidas de cibersegurança; operacionalizar a ciberdefesa. Para desempenhar as suas funções o BSI tem um orçamento de 197.16 milhões de euros (2021).

A terceira variável, uma comunicação clara e efetiva entre organizações de forma vertical e horizontal, porque para uma efetiva implementação é necessário que os objetivos do programa sejam entendidos pelos indivíduos que são responsáveis pela sua concretização. Podem ser utilizados incentivos como conselhos técnicos, sanções ou fundos extra. O papel do BSI como autoridade nacional de certificação de cibersegurança fez com que a engenharia tecnológica se tornasse um princípio da política de cibersegurança, por exemplo em infraestruturas obrigam a aplicar produtos de certificado nacional. Assim, também num grande número de categorias de produtos são especificadas pelo governo as medidas de segurança que devem ser tomadas, esses produtos requerem aprovação estatal com base em standard, normalmente desenvolvido pelo BSI. Os certificados só são emitidos por órgãos acreditados pelo BSI, que também investiga os produtos e serviços no mercado nacional e pode emitir avisos públicos por falta de segurança. O BSI pode aplicar sanções em conjunto com *Länder* (regional/distrital) e pode aplicar multas por transgressão das medidas do BSI Act e IT Security Act. Foi criado um regulamento de rótulos TIC de adesão voluntária, de forma a informar o consumidor e complementar o trabalho do BSI, o rótulo de segurança é só aplicado em produtos aprovados pelo BSI, que seguem os requisitos pormenorizados no BSI Act.

A quarta variável, uma estrutura formal e informal das organizações de implementação e as relações que têm com outras organizações. BSI é a entidade central de acreditação e certificação para segurança TIC alemã. Em relação às infraestruturas críticas que são sujeitas a supervisão federal no setor de energia, TIC e finanças, enquanto *Länder* supervisiona o setor de saúde, transporte e fornecimento de comida. As *Länder* trabalham em conjunto com o BSI, as zonas administrativas regionais têm unidades policiais e algumas com unidades de combate a cibercrime, mas em relação a cibersegurança na sua maioria deixam ao encargo do BSI. A estratégia de cibersegurança alemã têm quatro abordagens diferentes para cooperação público-privado em que podem se organizar por setor, plataformas para partilha de informação (por exemplo Organização de Cibersegurança Alemã DCSO), cooperação para uma cibersegurança

preventiva e disseminação de boas práticas de cibersegurança ao público. UP KRITIS é a parceria mais antiga, desde 2007, e importante para infraestruturas críticas. O BSI é responsável pela coordenação e administração da plataforma, a adesão é voluntária e opera com regulamentos legislativos que suportam a sua implementação.

A quinta variável, o impacto das condições económicas, sociais e políticas na política pública. A pandemia trouxe os seus impactos com uma crise económica de oferta e procura, mas como resposta a Alemanha tomou um conjunto de medidas para aumentar a liquidez (Bofinder et al 2020), mas também houve um avanço na digitalização de serviços e comércio, o que tornou necessário uma atualização da legislação de cibersegurança alemã com o IT Security Act 2.0, a maio de 2021. De forma a acompanhar o avanço da digitalização, dos novos ciberataques e aumentar a cibersegurança de infraestruturas ao incluir mais setores como gestão de resíduos, novas obrigações para componentes e companhias de interesse público.

A última variável, todos os componentes discutidos anteriormente têm de ser filtrados pelo implementador. Van Meter e Van Horn (1975) identificam três elementos de resposta do implementador que podem afetar a sua habilidade e consentimento de executar a política. Os elementos são a capacidade de conhecimento ou compreensão da política, a sua resposta perante a mesma (positiva, negativa ou neutra) e a intensidade dessa resposta. Os implementadores podem falhar em executar a política como é pretendida se for contra as crenças deles e/ou se tiverem uma disposição negativa e intensa, enquanto que uma atitude menos intensa pode levar a evasão. Na Alemanha a certificação já é utilizada há bastante tempo, com a criação de BSI em 1991 e do BSI Act em 2009, será apenas uma questão de transição de certificação nacional para a europeia. Na consulta pública anteriormente analisadas, as empresas alemãs que participaram foi sempre em favor de uma certificação europeia.

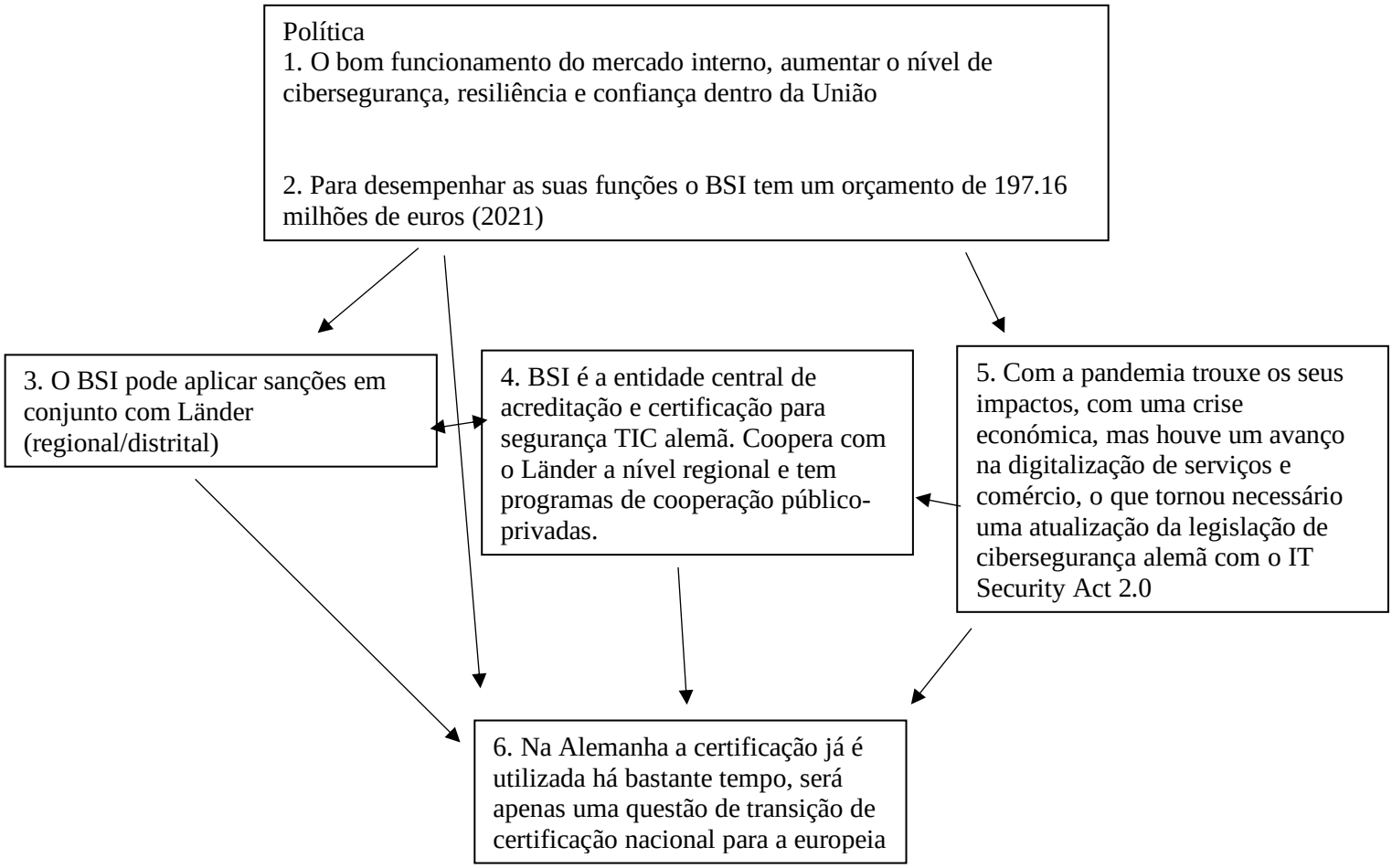

Figura 3. Modelo do processo de implementação política de Van Meter e Van Horn (1975)

Consoante os dados conseguidos pelos métodos podemos concluir se a implementação terá ou não sucesso. Vimos que há um bom entendimento do problema e as suas ramificações para o mercado e a economia europeia, mas com a existência de diferentes certificações e uso de standards é difícil criar requisitos mínimos de segurança, assim o consumidor tem menos confiança no mercado e baseia-se na reputação do vendedor ou preço, diminuindo também a capacidade de empresas europeias competirem com as multinacionais americanas.

Com a criação do SCCG há um continuo envolvimento da parte empresarial a estarem envolvido na criação de esquemas de certificação, os EM estiverem envolvidos no processo de integração e negociação do CSA, conseguindo moldar o regulamento à sua medida.

Uma dificuldade é o grupo alvo do CSA é extenso por a cibersegurança afetar um grande número de entidades – empresas, autoridades públicas e cidadãos, sendo necessário sensibilizar os cidadãos para a cibersegurança, as empresas partilharem informação sobre vulnerabilidades e uma mudança para o esquema de certificação europeu de forma harmoniosa. É provável que seja difícil de implementar todas essas medidas de forma abrangente, mas como a mudança de comportamento não é drástica. A sensibilização de cidadãos e partilha de vulnerabilidades está presente em várias estratégias europeias como eEurope 2002, NIS e EUCSS, são

comportamentos que têm sido constantemente reforçados, sendo a mudança mais dificil a transição de esquemas nacionais para europeus, em que é uma escolha de standard de forma supranacional em vez de nacional.

Os objetivos são dados de forma clara, mas a ENISA é um órgão europeu envolvido em vários projetos de cibersegurança, segundo Sabatier e Mazmanian (1983) se o CSA tiver pouca prioridade a implementação pode ficar atrasada.

Apesar de haver uma boa integração hierárquica entre Comissão, GECC e autoridades nacionais, os membros do GECC podem vetar sobre qualquer esquema que entendam que seja de soberania nacional, portanto a certificação é supranacional e intergovernamental até onde os EM permitem (Sivan-Sevilla 2020).

Na fase da implementação houve mudanças políticas na presidência da Comissão e mudanças socioeconómicas, que mudou o foco de cibersegurança para dar prioridade à saúde e resposta à nova crise económica. As respostas à crise são um crescimento ecológico e inovação digital que inclui cibersegurança. Porém com uma variação das condições socioeconómicas locais torna-se difícil uma implementação com êxito devido a haver menos recursos disponíveis.

A nível europeu no geral, com base no método que utilizei, a implementação do regulamento foi atrasada devido às dificuldades socioeconómicas e terá menos prioridade nas agendas nacionais em que agora o objetivo é ultrapassar a crise económica pós-pandemia, mas as propostas de esquemas de certificação continuam a ser desenvolvidas e vão substituir os esquemas nacionais. Para os EM que já tem autoridades nacionais de certificação a priori do regulamento será uma transição fácil, mas as que não têm será mais difícil por falta de experiência e conhecimento técnico para acreditar e monitorizar a implementação do regulamento. No caso alemão, como por exemplo, terá sucesso a implementar o regulamento por o BSI ser uma organização com bastantes anos e experiência e criaram incentivos nacionais para a utilização de standards, que foi um regulamento para rótulos TIC e a aplicação de sanções. A Alemanha também sentiu as mudanças económicas e sociais da pandemia, mas continuou a priorizar a cibersegurança, tal é visível na atualização do IT Security Act em 2021.

CAPÍTULO 5

Discussão: o reforço da resiliência ciber com o Cybersecurity Act

A economia foi, desde o início, o fator que impulsionou a cibersegurança e a tecnologia como área de investimento para combater a crise. Apesar disso, a política europeia de cibersegurança é um projeto incrementalista e cumulativo de eventos que vai ganhando força e velocidade com a evolução de ameaças exteriores. Portanto, o regulamento de cibersegurança é uma continuação da estratégia europeia que interceta com outras políticas e o sucesso ou insucesso da sua implementação vai afetar as restantes políticas europeias de cibersegurança.

A Diretiva NIS, que definiu requisitos mínimos de proteção para os EM e foi uma transição para políticas europeias de cibersegurança vinculativas, já encorajava o uso de standards internacionais. Aplicar standards relevantes para a cibersegurança é uma forma de demonstrar uma conduta responsável, em conformidade com a diretiva e uma cultura de gestão de risco. O RGPD interceta com o CSA em termos de privacidade, proteção de informação, *security by design* e utilização de certificação como um mecanismo de transparência. Para além disso, o RGPD incentiva também a criação de esquemas como forma de disseminação de boas práticas em privacidade e proteção de dados em todos os setores. Enquanto os esquemas do CSA são baseados em standard externos que não tem em mente os valores e o sistema legal e político que a União defende, a certificação do RGPD é estabelecida pelo EDPR, dando prioridade aos utilizadores e seguindo os valores europeus.

O CSA continua uma prioridade na estratégia de cibersegurança europeia de 2020 (COM 2020 456 final) ao adotar o primeiro URWP e com uma reforma da diretiva NIS para NIS2. Com uma continuação dos objetivos europeus de resiliência e soberania tecnológica, uma meta desde a Agenda Digital 2010 e a estratégia de cibersegurança europeia de 2013, existe o desejo de assegurar a viabilidade económica pela competitividade para não depender de operadores privados e estrangeiros para componentes e software, para transmitir segurança e promover o mercado único de produtos TIC, elevando assim o nível de segurança na UE ao incorporar requisitos de segurança nos produtos utilizados.

O regulamento de cibersegurança cria um único ponto de certificação resolvendo a fragmentação do mercado, diminui os custos e o tempo e aumenta os requisitos de segurança dos produtos. Estes são os resultados esperados com a aplicação do regulamento, mas vai

também aumentar a cibersegurança? Quais são os impactos nas políticas europeias de cibersegurança se não for implementado com sucesso?

No método de Sabatier e Mazmanian (1983), a razão que identificamos para a criação do esquema de certificação foi a fragmentação de certificados entre EM, recursos dispersos e falta de sensibilização para cibersegurança, que são razões económicas de proteção do mercado. A mesma razão aparece no elo causal, o regulamento como resposta à fragmentação de esquemas de certificação de cibersegurança. Concorda também Sivan-Sevilla (2020) que a certificação europeia foi criada com o objetivo de harmonizar o mercado para produtos de cibersegurança, ultrapassando a fragmentação nacional e criando certificados mutuamente reconhecidos na União. Tal é visível quando os objetivos do regulamento de cibersegurança são de assegurar o bom funcionamento do mercado interno e aumentar o nível de cibersegurança, resiliência e confiança dentro da União. Como a fragmentação de certificados afetou o mercado foi necessária uma abordagem europeia.

No método, os comportamentos necessários para alterar a forma de aplicar a política corretamente são sensibilizar os cidadãos, organizações e empresas para cibersegurança, divulgar vulnerabilidades entre empresas, órgãos e consumidores e uma transição harmoniosa e homogénea entre EM para a certificação europeia. A aplicação destas medidas iria aumentar a resiliência de cibersegurança europeia no geral. Ademais, segundo Blythe et al (2020) o consumidor está disposto a pagar por produtos IdC mais seguros, especialmente depois de se aperceberem das vulnerabilidades existentes nos produtos. Portanto, sensibilizar para a cibersegurança aumenta o seu uso, fomenta inovação e cria pressão de compra para produtos mais seguros. Contudo, para haver este aumento de resiliência de cibersegurança com a certificação, que ao seguir standards cria um nível de partida igual para todos os produtos, é necessário partir da ideia de que standards e normas criam um balanço entre as necessidades dos consumidores para proteção e mantêm a competitividade na indústria (Bendiek e Schallbruch 2019). Ademais, a certificação é tradicionalmente vista como um instrumento que oferece transparência e aumento de confiança para o objeto certificado e a organização. Além disso, reduz a assimetria de informação, facilita auditorias e garante que o vendedor, produtor ou provedor de serviços são fiáveis (Kamara 2020).

Segundo o método, os impactos esperados são de aumentar a capacidade de preparação dos EM e empresas para o uso de certificação e diminuir vulnerabilidades em infraestruturas ao criar um ponto de partida para cibersegurança implementando standards. O esquema de certificação estabelecido com o regulamento não vai diminuir a cibersegurança, uma vez que requer que sigam os standards, mas não protege os dados pessoais e privacidade dos utilizadores como o RGPD (Veldhoen 2019).

Segundo Schallbruch e Skierka (2018) a proposta é um passo em rumo a uma Europa uniforme em avaliação de segurança em produtos TIC, mas a medida voluntária fica abaixo das expectativas. A comissão não propôs nada sobre as responsabilidades dos produtores e provedores de serviços, dado que o esquema de certificação não indica como ultrapassar os problemas de certificação segura que são a rapidez, custo e o ciclo de vida. A velocidade do processo de certificação é mais longa que a velocidade de inovação técnica. Os esquemas de certificação requerem tempo e processos dispendiosos que podem ser um impedimento em mercados rápidos, como por exemplo em IdC onde há pouca margem de lucro. Com a evolução crescente da tecnologia e dos ciberataques, os desafios são exacerbados com crescente preocupação de segurança, mas com tempo de entrada no mercado limitado. Schallbruch e Skierka (2018) sugerem que devido a mudanças de riscos, vulnerabilidades e novos vetores de ataque, a certificação tem de ter um tempo limitado.

Como CSA é um regulamento voluntário a parte de fomentar a sua adesão foi deixada ao encargo dos EM. Alguns incentivos são a contratação pública e aplicação de sanções, como por exemplo no caso alemão, em que foi desenvolvido um regulamento de rótulos para TIC tornando visível para os consumidores o uso de certificado. A nível europeu os incentivos para a certificação são que ao aplicarem os esquemas estão em conformidade com a diretiva NIS e o RGPD por estarem a aplicar boas práticas de segurança, privacidade e proteção de dados. Devido a esta variante de incentivo à adesão, a integração é capaz de variar entre EM que criem incentivos ou não. Portanto, para além das diferenças das capacidades de certificação entre EM e dos que já tinham autoridades nacionais, vai também haver diferenças a nível industrial e competitividade, havendo a possibilidade de voltar a repetir-se o que aconteceu com a Diretiva NIS – uma discrepância de incrementação entre EM, devido à falta de conhecimento técnico para acreditar e monitorizar a implementação do regulamento e também monitorizar o cumprimento das obrigações por parte das empresas.

Nas conclusões obtidas pelo método utilizado, no geral a implementação foi atrasada devido às dificuldades socioeconómicas e mudanças de prioridades com a pandemia. Mas as propostas de esquema de certificação continuam a ser desenvolvidas (EUCC e EUCS para

cloud). A aplicação do CSA vai resolver a fragmentação do mercado de certificados de cibersegurança, portanto, o nível de cibersegurança no produto é apresentado de forma transparente. Se não for efetivamente implementado não vai aumentar a confiança nos produtos TIC europeus nem aumentar a resiliência europeia, dificultando os objetivos europeus de competitividade no mercado, a contínua evolução tecnológica e levando ao enfraquecimento do papel da União como ator no ciberespaço. Concluindo a implementação do CSA, a nível europeu, vão existir alguns problemas por tentar obter resultados de forma abrangente, por falta de prioridade na agenda de ENISA e por alguns atrasos com as mudanças socioeconómicas da pandemia, mas esta variante de incentivo ou não incentivo é importante para o aumento de cibersegurança. Se as empresas não aderirem ao esquema de certificação de cibersegurança europeu não vão aplicar os standards e não vai haver aumento de cibersegurança no produtos.

CAPÍTULO 6

Conclusões

O incentivo inicial para as políticas de cibersegurança europeias foi de foro económico, com o aumento da complexidade das ameaças e ciberataques que sensibilizaram o público e os políticos para a proteção da economia, infraestruturas críticas, sociedade e empresas. Como resultado, foram criadas estratégias abrangentes como o EUCSS, que envolve cibercrime, ciber defesa e infraestruturas críticas, e vinculativas como NIS que estabelece requisitos mínimos para infraestruturas críticas. No pacote de medidas de 2017 houve a criação de novos instrumentos para ciberataques de grande escala, melhor presença diplomática europeia em cibersegurança com CDT, fortalecimento de ENISA com CSA e criação de um esquema de certificação.

Qualquer que seja a causa da criação do CSA, ele pode ser um projeto incrementalista cumulativo de eventos, que ganha força com a evolução de ameaças exteriores (Christou 2019), ou simplesmente um caso de integração do mercado, que pretende criar um mercado para produtos certificados e integração de poderes estatais ao mobilizar capacidades de estabelecer standards e certificar infraestruturas sensíveis nacionais (Sivan-Sevilla 2020).

O objetivo do trabalho foi estudar o impacto do regulamento de cibersegurança no aumento de cibersegurança. Do ponto de vista legislativo, a certificação tem de lidar com regulamentos, leis e diretivas na área de cibersegurança, do ponto de vista técnico há diversos tipos de certificação para setores específicos circunscrito em espaços económicos ou nacionais, impedindo uma harmonização (Matheu et al 2020). A Comissão notou que estavam a emergir múltiplas iniciativas nacionais para aumentar o nível de segurança em TIC, construindo esquemas nacionais de certificação. Antes do presente regulamento, o fornecimento de produtos TIC no mercado único europeu era fragmentado e levantava problemas de interoperabilidade. O regulamento cria um ponto único de certificação resolvendo a fragmentação do mercado, tornando o processo mais fácil, diminuindo custos e tempo, por já ser preciso certificar em vários países, e aumentando os requisitos de segurança dos produtos adicionando alguns anteriormente não reconhecidos. Mas isto só se vai aplicar quando todas as categorias de produtos certificados por esquemas nacionais passarem para esquemas europeus (Veldhoen 2019).

A nível técnico, o regulamento de cibersegurança vai estabelecer requisitos mínimos com standards ao ter um nível mínimo de partida igual para todos, aumentando a resiliência, e ao

sensibilizar para cibersegurança aumenta o uso de produtos certificados por ser mais seguro e transparente. A certificação europeia vai aumentar o nível de cibersegurança e de confiança dos consumidores, mas vai também impor uma barreira não tarifaria no comércio tecnológico (Minárik e Alatalu).

A nível político, como esquema de certificação de cibersegurança europeu que tem um processo de estandardização supranacional e uma acreditação reconhecida por todos os EM, vai aumentar a influência da Comissão e dar um papel central às instituições europeias a longo prazo. O esquema de certificação de cibersegurança europeu vai ter relevância global devido ao tamanho do mercado europeu. O RGPD e o CSA são instrumentos para a UE exercer a sua soberania digital, sinalizando que a União tem o direito de determinar como os produtos e serviços são feitos e usados com base nos princípios constitucionais, democráticos e um balanço de interesse dos participantes. Foi através do RGPD que a UE demonstrou que está numa posição independente para estabelecer standards e de assegurar a sua implementação pela Europa e além, como o Japão e a Índia, que estão alinhados com a lei europeia em proteção de dados (Bendiek e Schallbruch 2019).

A cibersegurança tem sido analisada de vários ângulos, mas uma análise política, especialmente de estudos europeus tem sido limitada. Este estudo tentou adicionar à literatura sobre política europeia de cibersegurança com uma análise do regulamento de cibersegurança. Apenas os estudos de Kamara (2020) e Veldhoen (2019) comparam CSA com o RGPD e Sivan-Sevilla (2020) analisa a certificação europeia no seu total.

Kamara (2020) conclui que o CSA é um instrumento de mercado para aproximar as leis para estabelecer um mercado interno funcional, enquanto o RGPD protege os indivíduos e o processamento dos seus dados pessoais. A interação entre os dois regulamentos pode se manifestar em critérios comuns, reconhecimento parcial comum, avaliação e acreditação conjunta. São necessários canais de comunicação para evitar impactos negativos e proteger os valores. Do mesmo pensamento é Veldhoen (2019), que diz que a função principal do RGPD é proteção da informação, dos dados e o livre movimento de informação. Portanto, mantém as suas certificações de livre interpretação para poder acompanhar as evoluções tecnológicas. O esquema do CSA é excelente para produtores e provedores de serviço, mas protege menos os consumidores. Sivan-Sevilla (2020) diz que a segurança é um tópico relevante para consumidores e produtores no mercado, no qual o CSA representa uma tentativa de práticas de integração de mercado num tópico sensível de defesa nacional.

Referências Bibliográficas

Avast Smart Home Security Report 2019, disponível em: https://cdn2.hubspot.net/hubfs/486579/avast_smart_home_report_feb_2019.pdf (consultado a 05/02/21);

Bangemann Report to European Council May 1994, COM (1994) 347;

Barbas, J. M. A., & Sancho Hirane, C. (2018). Cibersegurança e políticas públicas análise comparada dos casos chileno e português. IDN Cadernos nº29;

Barrinha, A. (2020). Chapter 6: European security in cyberspace. Emerging Security Technologies and EU Governance: Actors, Practices and Processes, edited by Calcara, A., Csernatoni, R., & Lavallée, C.;

Bendiek, Annegret (2012), European cyber security policy, SWP Research Paper, volume 13;

Bendiek, A., Bossong, R., & Schulze, M. (2017). The EU's Revised Cybersecurity Strategy: Half-Hearted Progress on Far-Reaching Challenges. Disponível em: https://www.swp-berlin.org/fileadmin/contents/products/comments/2017C47_bdk_etal.pdf

Bendiek, A., & Schallbruch, M. (2019). Europe's third way in cyberspace: what part does the new EU Cybersecurity Act play?. Disponível em: https://nbn-resolving.org/urn:nbn:de:0168-ssoar-67207-2 (consultado a 08/02/2021);

Bertino, E. (2019, December). IoT Security A Comprehensive Life Cycle Framework. In 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC) (pp. 196-203). IEEE.

Blythe, J. M., Johnson, S. D., & Manning, M. (2020). What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices. Crime Science, 9(1), 1-9;

Bossong, R., & Wagner, B. (2017). A typology of cybersecurity and public-private;

Carrapico, H., & Barrinha, A. (2017). The EU as a coherent (cyber) security actor?. JCMS: Journal of Common Market Studies, 55(6), 1254-1272;

Carrapico, H., & Barrinha, A. (2018, May 27). European Union cyber security as an emerging research and policy field. European Politics and Society. Routledge;

Cavelty, Myriam Dunn (2010). Cyber-security. The routledge handbook of new security studies, 154-162;

Cavelty, Myriam Dunn. (2015). Cyber-security, Contemporary Security Studies, Edition: 4th, Chapter: 27, Publisher: Oxford University Press, Editors: Alan Collins, pp.400-416;

Christou, G. (2016). Cybersecurity in the European Union: resilience and adaptability in governance policy. Springer;

Christou, G. (2019). The collective securitisation of cyberspace in the European Union. West European Politics, 42(2), 278-301;

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. Technology Innovation Management Review, 4(10), 13–21.

Commission Staff Working Document, Advancing the Internet of Things in Europe Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Digitising European Industry Reaping the full benefits of a Digital Single Market, SWD/2016/0110 final;

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM(2016)410, 05/07/2016;

Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, A Hora da Europa: Reparar os Danos e Preparar o Futuro para a Próxima Geração, COM(2020) 456 final, 27.5.2020;

Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões Estratégia da União Europeia para a cibersegurança: *Um ciberespaço aberto, seguro e protegido* / JOIN/2013/01 final, 7.2.2013;

Comunicação da Comissão, de 12 de dezembro de 2006, relativa a um Programa Europeu de Protecção das Infra-Estruturas Críticas, COM (2006)786 final;

Communication from the Commission to the European Parliament, the council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, 'Achievements and next steps: towards global cyber-security', COM (2011) 163 final;

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, COM/2015/0192 final;

Compagnucci, Silvia (2021), The new European Cybersecurity Strategy: objectives and opportunities, disponível em: https://www.i-com.it/en/2021/02/05/the-new-european-cybersecurity-strategy-objectives-and-opportunities/ (consultado a 13/07/2021);

Conferência The European Paradigm for a safer digital world, disponível em https://www.youtube.com/watch?v=6s2ec8k8Uc4 consultado a 15/01/2020);

Council of the European Union (2005) 'Council Framework Decision on Attacks against Information;

Cymutta, Sebastian (2020), National Cybersecurity Organisation: GERMANY, National Cybersecurity Governance Series, NATO CCDCOE;

Dewar, R. S. (2017). Cyber security in the European Union: an historical institutionalist analysis of a 21st century security concern (Doctoral dissertation, University of Glasgow);

The Digital Europe Programme, disponivel em : https://digital-strategy.ec.europa.eu/en/activities/digital-programme (consultado a 25/11/21);

Diretiva do Parlamento Europeu e do Conselho relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, COM (2013) 48 final;

Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União;

Downs, A. (1972), Up and down with ecology: The issue-attention cycle in Agenda Setting: Readings on Media, Public Opinion, and Policymaking, edited by Protess, D. and McCombs, M, Routledge, pp 27-34;

ENISA (2017). Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, disponivel em: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot (consultado a 13/07/21);

ENISA (2017) Considerations on ICT security certification in EU - Survey Report, disponivel em: https://www.enisa.europa.eu/publications/certification_survey (consultado a 13/02/21);

ENISA (2017) Recommendations on European Data Protection Certification, disponivel em: https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification/ (consultado a 12/02/21);

ENISA (2020), EUCS – Cloud Services Scheme: EUCS, a candidate cybersecurity certification scheme for cloud services, disponível em: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme (consultado a 08/08/21);

ENISA (2021), Public Consultation on the draft candidate EUCC scheme: Report on Public Consultation, disponível em: https://www.enisa.europa.eu/publications/enisa-report-public_consultation-on-the-draft-candidate-eucc-scheme (consultado a 08/08/21);

ENISA Single Programming Document 2021-2023, disponivel em: https://www.enisa.europa.eu/publications/corporate-documents/enisa-single-programming-document-2021-2023 (consultado a 12/08/21);

European Commission, Have your say, disponível em: https://ec.europa.eu/info/law/better-regulation/have-your-say_en (consultado a 12/01/20);

European Commission, (1985). COM (85) 310 final Completing the Internal Market: White Paper from the Commission to the European Council (White Paper No. COM (85) 310 final). European Commission, Brussels;

European Commission, (1992). COM (92) 24 Final Commission Proposal for a Council Directive on the legal protection of databases. COM (92) 422 Final Commission proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

European Commission, (1996). COM (96) 487 Illegal and Harmful Content on the Internet;

European Commission (2004) 'Communication from the Commission to the Council and the European Parliament: Critical Infrastructure Protection in the Fight Against Terrorism', COM (2004) 702 final, 20 October;

European Commission, (2006). COM (2006) 251 Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - A Strategy for a Secure Information Society – "Dialogue, partnership and empowerment.";

European Commission (2010). A Digital Agenda for Europe, COM(2010)245 final;

European Commission (2011). Roadmap 'Proposal on a European Strategy for Internet Security', November 2011;

European Comission, EUROPE 2020 A strategy for smart, sustainable and inclusive growth, COM/2010/2020 final, Brussels, 3.3.2010;

European Court of Audits (2019), Briefing Paper: Challenges to effective EU Cybersecurity Policy;

The EU's Cybersecurity Strategy in the Digital Decade, factsheet disponivel em: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade (consultado a 15/09/21);

European Parliament and Council of the European Union (2009). Directive 2009/ 140/EC of the European Parliament and of the Council of 25 November 2009 Amending Directives 2002/21/EC, 2002/19/EC and 2002/20/EC;

Minárik, Tomáš e Alatalu, Siim, EU Cybersecurity Package: New Potential for EU to Cooperate with NATO, no site da CCDCOE, disponivel em: https://ccdcoe.org/news/2017/eu-cybersecurity-package-new-potential-for-eu-to-cooperate-with-nato/ (consultado a 10/09/21);

Felkner, A., Kadobayashi, Y., Janiszewski, M., Fantin, S., Ruiz, J. F., Kozakiewicz, A., & Blanc, G. (2020). Cybersecurity Research Analysis Report for Europe and Japan.

Full report on the public consultation on the evaluation and review of the European Union Agency for Network and Information Security (ENISA), disponível em: https://ec.europa.eu/digital-single-market/en/news/full-report-public-consultation-evaluation-and-review-european-union-agency-network-and (consultado a 18/08/20);

Geraldes, S. M. (2019). A estratégia de cibersegurança da União Europeia: catastrofista, realista e/ou otimista?. Nação e Defesa, N.º 154, pp. 91-108;

Internet Society (2018), IoT Security for Policymakers, disponível em: https://www.internetsociety.org/resources/2018/iot-security-for-policymakers/ (consultado a 15/06/21);

Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final;

Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. 13.9.2017. JOIN/2017/0450 final;

Kamara, I. (2020). Misaligned Union laws? A comparative analysis of certification in the Cybersecurity Act and the General Data Protection Regulation;

Kammel, Arnold (2018), Cyber resilience as a key challenge for the EU and its Member States. Em Rehrl, Jochen, Handbook on Cyber Security, European Security and Defence College; Federal Ministry of Defence of the Republic of Austria;

Karniyevich, N. & Niemann, F. (2021), The German IT Security Act 2.0 comes into force – Overview of the most significant changes to the BSI Act, site Bird&Bird, disponível em: https://www.twobirds.com/en/news/articles/2021/germany/the-german-it-security-act-2-0-comes-into-force (consultado a 18/08/21);

Klimburg, A., & Tirmaa-Klaar, H. (2011). Cybersecurity and cyberpower: concepts, conditions and capabilities for cooperation for action within the EU. European Parliament;

Latici, T., Cyber: How Big Is The Threat?, European Parliamentary Research Service Blog, disponível em: https://epthinktank.eu/2019/07/10/cyber-how-big-is-the-threat/

Liaropoulos, A. (2021). EU Digital Sovereignty: A Regulatory Power Searching for its Strategic Autonomy in the Digital Domain. In ECCWS 2021 20th European Conference on Cyber Warfare and Security (p. 246). Academic Conferences Inter Ltd.

Liveri, D., Sarri, A., & Darra, E. (2018). ENISA's Contribution to National Cyber Security Strategies. In Cybersecurity Best Practices (pp. 43-64). Springer Vieweg, Wiesbaden;

Mansell R. (2014) Here Comes the Revolution — the European Digital Agenda. Em: Donders K., Pauwels C., Loisen J. (editores) The Palgrave Handbook of European Media Policy. Palgrave Macmillan, London.

Markopoulou, D., Papakonstantinou, V., & de Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. Computer Law & Security Review, 35(6);

Matheu, S. N., Hernández-Ramos, J. L., Skarmeta, A. F., & Baldini, G. (2020). A Survey of Cybersecurity Certification for the Internet of Things. ACM Computing Surveys (CSUR), 53(6), 1-36.

Mitrakas, A. (2018) The emerging EU framework on cybersecurity certification. Datenschutz Datensich 42, 411–414;

Minárik, Tomáš and Alatalu, Siim, EU Cybersecurity Package: New Potential for EU to Cooperate with NATO, CCDCOE, disponível em: https://ccdcoe.org/news/2017/eu-cybersecurity-package-new-potential-for-eu-to-cooperate-with-nato/ (consultado a 15/07/21);

Moret, E., & Pawlak, P. (2017). The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?. European Union Institute for Security Studies (EUISS);

NIS Cooperation Group, Sectorial implementation of the NIS Directive in the Energy sector, Report - CG Publication 03/2019;

Nyikes, Z (2021). The Cybersecurity Challenges of COVID-19, in IPSI Transactions on Advanced Research, ISSN 1820 – 4511, Vol. 17, No. 2, pp. 57-62, July 2021;

Pan, J., & Yang, Z. (2018, March). Cybersecurity Challenges and Opportunities in the New" Edge Computing+ IoT" World. In Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization (pp. 29-32).

Paul, S., & Mishra, S. (2020). Cyber Security in Terms of IoT System and Blockchain Technologies in E-Healthcare Systems. Green Computing and Predictive Analytics for Healthcare, p. 115- 144.

Pawlak, Patryk e Biersteker, Thomas (2019), Chaillot Paper 155, Guardian of the Galaxy: EU cyber sanctions and norms in cyberspace, European Union Institute for Security Studies (EUISS);

BSI perfil e dados gerais, disponível em: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/BSI-Kurzprofil/kurzprofil_node.html (consultado a 10/09/21);

Press Release Comissão Europeia, New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient, disponivel em: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391 (consultado a 25/08/21);

Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à ENISA, a «Agência da União Europeia para a Cibersegurança», e à certificação da cibersegurança das tecnologias da informação e comunicação, e que revoga o Regulamento (UE) n.º 526/2013 («Regulamento Cibersegurança»), COM(2017) 477 final, 13.09.2017;

Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, Official Journal L 077, 13/03/2004;

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, 27 de abril de 2016;

Rose K., Eldridge S. and Chapin L. (2015), The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World, Internet Society;

Revised Directive on Security of Network and Information Systems (NIS2), disponível em: https://digital-strategy.ec.europa.eu/en/library/revised-directive-security-network-and-information-systems-nis2 (consultado a 10/09/21);

Rozbicka, P. (2013). Advocacy coalitions: influencing the policy process in the EU. Journal of European Public Policy, 20(6), 838-853;

Ruiz, José (2021), Cybersecurity certification in Europe, 2 years of the Cybersecurity Act, blog jtsec, disponível em: https://www.jtsec.es/blog-entry/90/cybersecurity-certification-in-europe-2-years-of-the-cybersecurity-act (consultado a 02/10/21);

Ruohonen, J., Hyrynsalmi, S., & Leppänen, V. (2016). An outlook on the institutional evolution of the European Union cyber security apparatus. Government Information Quarterly, 33(4), 746-756;

Sabatier, P. A. (1998). The advocacy coalition framework: revisions and relevance for Europe. Journal of European public policy, 5(1), 98-130;

Sabatier, P and Mazmanian, D (1983), Implementation and Public Policy with a New Postscript, University Press of America;

Schallbruch, Martin, Skierka, Isabel (2018), Cybersecurity in Germany. Springer International Publishing;

Schatz, D., Bashroush, R., & Wall J. (2017). Towards a More Representative Definition of Cyber Security. Journal of Digital Forensics, Security and Law, 12(2);

State of The Union 2017, 13 setembro, disponível em: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3193 (consultado a 10/01/20);

Symantec, Internet security threat report, volume 24, fevereiro de 2019;

Symantec, Threat Landscape Trends – Q1 2020, disponivel em: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/threat-landscape-q1-2020 (consultado a 10/03/21);

Tiirmaa-Klaar, Heli (2018), Two generations of EU cybersecurity strategies. Em Rehrl, Jochen, Handbook on Cyber Security, European Security and Defence College; Federal Ministry of Defence of the Republic of Austria;

Van Meter, D. S., & Van Horn, C. E. (1975). The policy implementation process: A conceptual framework. Administration & Society, 6(4), 445-488;

Weber, R. H., & Studer, E. (2016). Cybersecurity in the Internet of Things: Legal aspects. Computer Law & Security Review, 32(5), 715-728.

Y.E.S 2018, EUISS Yearbook of European Security;

Anexos A

A consulta pública realizada de 18 de janeiro a 12 de abril de 2017 sobre a avaliação do desenvolvimento de ENISA durante o mandato de 2013-2016. O relatório de avaliação contém duas estruturas, uma parte é de avaliação das atividades desenvolvidas nos últimos anos e a segunda parte é de como pode a organização evolui e as suas necessidades em cibersegurança. Estas consulta teve no total 90 respostas, 88 ao questionário e dois position papers. O tipo de participantes foram autoridades nacionais (Irlanda, Itália, França, Grécia), empresas e associações privadas (Deutsche Telekom, Telefonica, Palo Alto Networks, Data Security Solutions, Vodafone, Symantec, S21sec, CAIXABANK, Ericsson, Schnedermann Software Consulting.), ONG (NESSI, CEPS, Kosiuszko Institute, EuroSmart, Digital Europe, European Banking Federation, Orgalime), academia (Center for IT-Secuiry, Privacy and Accountability), e indivíduos. Sendo um total de 15 estados-membros e 27 do setor privados representados nesta consulta. Na resposta a segunda metade do relatório de quais são as necessidades na política ciber europeia e se ENISA pode responder a essas necessidades, 84 responderam. Na primeira questão, de quais serão as maiores necessidades nos próximos 10 anos no setor de cibersegurança, 48 responderam cooperação entre os estados-membros, 44 a capacidade de prevenir, detetar e resolver ataques cibernéticos de grande escala. Também perguntaram aos participantes as áreas em que ENISA podia ter impacto e as áreas em que não teria. Nas que não teria identificaram harmonização de standards e a certificação de produtos TIC e serviços (figura 2). Os participantes vêm ENISA como um órgão para fomentar cooperação entre organismos e estados, sendo essa opção que obteve mais respostas. Entre os participantes dos 84 que responderam a segunda parte, apenas 23 votaram a favor da certificação, dos quais – 8 autoridades nacionais, duas ONGs, 9 privado e consultoria, 2 académicos e 2 pareceres individuais.

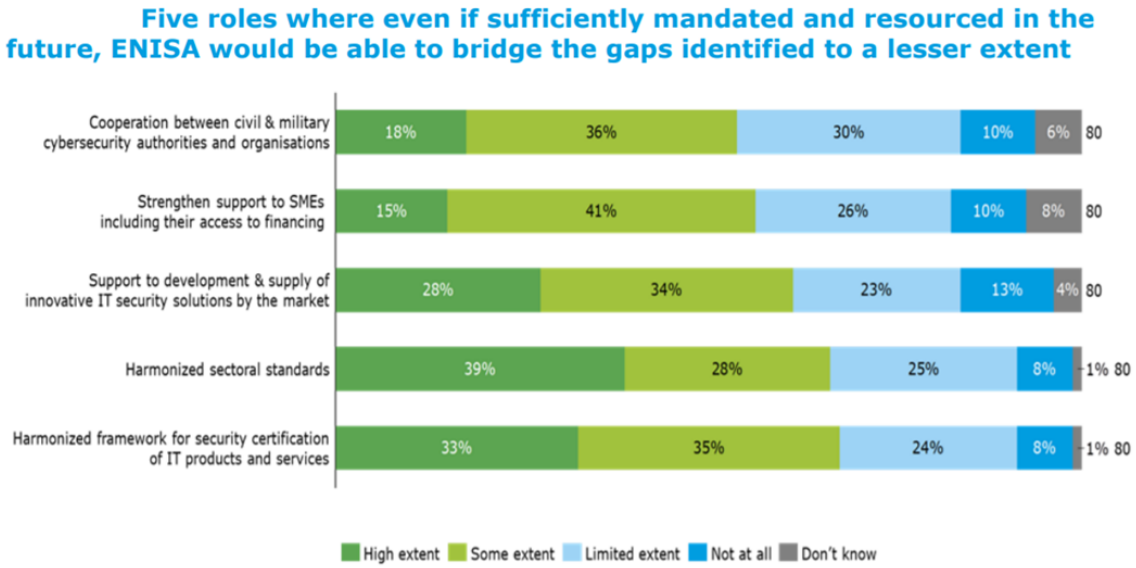

Figura 4 Áreas nas quais ENISA teria dificuldade em ajudas, retirado do Full report on the public consultation on the evaluation and review.

A consulta publica realizada de 7 de julho a 4 de agosto do roadmap para receber a opinião em relação a certificação de cibersegurança a nível europeu. Os catorze participantes desta consultas são todos empresas de várias dimensões. Apresentam opções preliminares para o futuro de ENISA e certificação de cibersegurança europeia. ENISA – opção 0 extensão da duração continuando tudo igual; opção 1 terminar a agência; opção 2 melhorar ENISA com novas competências e funções junto dos EM, CSIRT e esquema de certificação; opção 3 capacidades operacionais na prevenção, detetar, mitigação e resposta a ciberameaças. Dos catorze participantes seis deram a sua opinião sobre ENISA, dos quais cinco escolheram a opção 2 e um escolheu a 3. Como justificação deram que se ENISA tivesse capacidades operacionais interferia com as competências de CSIRT. As opções preliminares apresentadas para certificação de cibersegurança europeia foram: opção 1 encorajar a mais EM aderirem ao SOG-IS e suportar iniciativas industriais de setor específico; opção 2 propor um esquema europeu de certificação de cibersegurança como um instrumento legislativo, introduzindo novos requisitos de segurança para produtos e serviços TIC, com diferentes níveis de segurança (baixo, médio, alto); opção 3 legislação de segurança em TIC baseado na New Legislative Framework de 2008 , necessário adotar novos instrumentos e torna mandatório os requisitos de harmonização e mecanismos de avaliação de conformidade para garantir a segurança de produtos e serviços em específico. Todos os catorze participantes comentaram sobre certificação, onde doze escolherem uma das opções, sete escolheram a opção 3, três escolherem

a opção 1 e dois escolheram a opção 2. Os dois que não votaram em nenhuma das opções a justificação dado foi que certificação é um coisa estática enquanto que a tecnologia e a cibersegurança está em constante evolução. A certificação ia dar um falso sentimento de segurança, no mínimo os produtos iam ser seguros a entrar no mercado, mas sem ter em conta como iam ser utilizados ou em que ambiente tornam-se inseguros. Os que escolherem a opção 1 foi com medo de que com certificação de instrumento legislativo ia restringir a inovação tecnológica, sendo melhor ficar como iniciativa do mercado com aplicação de standards e requisitos de segurança caso a caso.

Na consulta pública de setembro a dezembro de 2017 para comentar sobre a proposta de regulamento de cibersegurança e esquema de certificação de cibersegurança europeu, houve 32 respostas. Os participantes na sua maioria são empresas. Todos os participantes concordam com a reforma de ENISA e de ter um mandato permanente. Sobre certificação 30 pessoas comentaram com 73% em favor de um esquema europeu de cibersegurança dando sugestões de ser baseado em esquemas internacionais, de incluir empresas no desenvolvimento de esquemas, esquemas flexíveis e resilientes para não limitarem a inovação, harmonizar requisitos de segurança, manter uma certificação voluntaria e tornar-se mandatório por iniciativa do mercado. Alguns dos participantes pedem especificações do alcance e de como vai ser feita a transição dos esquemas nacionais para europeus. 10% são da opinião que SOG-IS e CC é um esquema de grande sucesso que também é usado fora da europa, usado em nível elevado de segurança, não devia ser retirado apenas adaptar o tempo e o custo ao risco de segurança. 10% diz que não é necessário o esquema de certificação de cibersegurança europeu por já existir legislação interna de mercado (New legislative Framework) que tem em conta patentes nos produtos, deixar os órgãos europeus de standard criar standards e reconciliar requisitos técnicos que já tem representação da indústria.

No questionário feito a ENISA a maio de 2017 foram identificados os problemas de certificação 72% diz ser o custo, 57% a longa duração e falta de reconhecimento mútuo 51%. 90% dos questionados concorda que é necessário um reconhecimento mútuo de certificação a nível europeu. 81% concorda que certificação e rótulos é um instrumento efetivo para aumentar a transparência do nível de segurança de produtos e serviços TIC. 66% concorda que certificação própria é um opção viável. 90% indica que processos de certificação de segurança devem ser melhorados para assegurar flexibilidade ao permitir vários níveis de segurança. 66% em favor de um novo rotulo comum para cibersegurança, mas a nível sectorial para ser menos complexo.

PME em resposta a um questionário sobre existência de várias certificações em TIC representa uma barreira para a entrada no mercado por ter elevados custos, da mesma opinião na consulta publica de cPPP (dezembro 2015 a março 2016) é uma barreira para a entrada no mercado devido a custos de conformidade com as várias certificações e deve ser evitado uma maior fragmentação. Porque os esquemas existentes não suportam a indústria europeia (37% teve essa opinião). No mesmo questionário a PME, 76% acredita que um esquema europeu de certificação de cibersegurança vai facilitar o acesso de PME a contratação publica. 65% diz que uma certificação europeia simplifica procedimentos e custos administrativos.