

**BORDER SECURITY GOVERNANCE.
DIACHRONIC AND SYNCHRONIC ANALYSIS²³**

Krasimir Kornazhev, PhD Student

Department of European Studies
and International Security
University of Ruse, Bulgaria
E-mail: kornazhev@mail.bg

***Abstract:** The paper analyzes the three approaches in the history of border security governance, i.e. the traditional, the integrated and the most recent one, known as smart borders. The third approach complements integrated management practices with new tools, approaches and actions through large-scale digitalisation. It is argued, that the changes that have taken place are of a fundamental nature - border security is becoming identity management. It collects and analyzes biometric data for persons wishing to visit the territory of a country. Biometric characteristics, and in particular fingerprints, are unique in their physical nature to each individual, they allow automated recognition and are therefore reliable as carriers of specific information, they are virtually impossible to falsify. At the same time such a massive collection of private data raises a lot of questions.*

***Key words:** EU, border security governance, border management, smart borders*

***JEL Code:** F52*

УВОД

Управлението на граничната сигурност е пряко свързано с една от най-значимите ценности на една държава, а именно – нейния суверенитет. С еволюцията на държавното управление, чрез което функционира суверенитетът, еволюира и управлението на сигурността на границите. Сигурните граници в съвременния свят са свързани с регионалната интеграция, глобалната интеграция и ефектът на детериториализацията на границите.

Тази разработка е част от дисертационен труд, посветен на управлението на границите на Европейския съюз, и защитава тезата, че всяка геополитическа трансформация води до стратегическа промяна и в управлението на сигурността на границите. Изследователската цел се постига чрез диахронен и синхронен анализ, базиран на наблюдение²⁴ и на селектирани вторични данни.

ЕТАПИ В РАЗВИТИЕТО НА ПОЛИТИКИ ЗА СИГУРНОСТ НА ГРАНИЦИТЕ

Първият етап в развитието на политики за сигурност на границите в Европа можем да разделим условно на два периода - от античността до средата на XVII век и от Вестфалският мирен договор през 1648 г. до XX век.

Най-ранните представи за граници са естествените природни прегради – речни и морски басейни, труднодостъпни гористи и планински местности, необитаеми пространства. Те са с аморфен и символичен характер. Впоследствие се появяват различни гранични съоръжения, които затрудняват и възпират евентуални нападения. Най-известни в Европа са тези по границите на Римската империя (напр. Limes Germanicus и др.), а в Азия - Великата китайска стена. Границите са достатъчно условни и динамични предвид честата им промяна в резултат

²³ Разработката е представена на конференцията на Русенски университет и Съюза на учените със заглавие на български език Управление на сигурността на границите. Диахронен и синхронен анализ.

²⁴ Авторът е директор на Регионалната дирекция “Гранична полиция” – Русе (която управлява сигурността на границата между Р България и Румъния) и ръководи процесите на промяна в контекста на присъединяване на двете страни към ЕС и към Шенгенското пространство от 2005 до 2010 г.

на непрекъснато водените войни, те са несигурни и по тази причина се създават и градски граници, ограждащи с крепостни стени обитаваната територия.

С Вестфалския мирен договор от 1648 г., слагащ край на изтощителната Тридесетгодишна война, се формулират принципите на държавния суверенитет и се признават взаимно суверенни държави – Европа става континент на суверенни държави. Защитата на държавните граници се превръща в приоритетна политическа цел.

По време на Първата световна война поради съображения за сигурността на държавата се въвеждат задължителни изисквания за наличие на паспорти и се извършва контрол на преминаващите през границите. Оттогава той се запазва и усъвършенства чрез стандартизиране и унифициране на процедурите. Създават се специализирани места за преминаване на държавните граници и извършване на проверките – гранични контролно-пропускателни пунктове.

През вековете традиционният модел за гранично управление се е променял и преформулирал съобразно политическите трансформации на обществените отношения и развитието на транспортните системи и технологиите, но функционално съхранява същността си до днес.

Основно предизвикателство при традиционното управление на границите е постигането на баланс между целта за превенция и противодействие на заплахи/престъпна дейност и осигуряване на ресурсите за постигане на целта. Особена роля играе и менталната нагласа за образ на врага отвъд граничната линия.

Вторият етап²⁵ в развитието на политики за сигурност на границите представлява развитие на системата за сигурност и усъвършенстване на традиционните методи, средства и способности за управление. Основната му характеристика е интегрираното гранично управление (ИГУ), което надгражда традиционното управление. ИГУ се реализира хоризонтално и вертикално на три нива – **вътрешноведомствено сътрудничество, междуведомствено сътрудничество и международно сътрудничество**.

Факторите, които катализират появата на ИГУ, са външни и вътрешни.

На първо място от външните е вълната на *глобализацията* и *регионализацията* в международните отношения започнала през втората половина на ХХ в. Глобализацията трансформира политическите, икономическите, технологичните, комуникационните, социалните, културните и други връзки между държавите, институциите и хората във връзки на едно световно общество²⁶. Основният ѝ ефект е в невиджданото до този момент лавинообразно увеличение на мобилността на хора, стоки, услуги, капитали и идеологии. Нейната флуидна природа е антигранична и проявленията ѝ са безгранични. Тя не се съобразява с границите, „прекосява“ ги без да е „нарушител“ и на практика ги заличава и обезсмисля. Същевременно регионалното сътрудничество на различни плоскости предшества глобалното сътрудничество, но в много отношения е и негов контрапункт доколкото регионалният интегритет има потенциал за ограничаване на неблагоприятните ефекти на глобализацията. Най-важното негативно следствие, рефлектиращо пряко към управлението на сигурността на границите, е драстичното увеличение на миграционния поток и транснационалната престъпност включително и внос/износ на тероризъм.

Другият основен външен фактор е *детериториализирането* на границите. Детериториализацията на границите се свежда до условното преместване в пространствено-времеви дискурс на границите, разбираани в контекста на строго определена физическа разделителна линия. Границата не изчезва, не се заличава и остава константна с нейните обичайни контролни и проверовъчни дейности. Но традиционните и утвърдени гранични практики все по-трудно могат да отговорят адекватно на новопоявилите се глобални заплахи и рискове, особено на тероризма и миграционния натиск. За повишаване на ефективността на граничната сигурност все повече се разчита на разузнавателни способности и предварителни

²⁵ Анализът на втория и третия етап се базира на наблюдения на автора като участник в процесите на промяна на българо-румънската граница след падането на Берлинската стена.

²⁶ Вж. Albrow, M., 1990, с.8

проверки, които имат за цел да доставят на оторизираните служби достоверна и надеждна информация за лицата/обектите много преди да се явят за контрол на физическата граница. Детериториализираните граници по същество се превръщат във *виртуализирани* граници и дейностите по тях доминират и предхождат традиционните проверки на физическите граници. Основните приоритети са мерките в трети страни и страните на произход, транснационалното сътрудничество и сътрудничеството на държавните институции включително и взаимодействие с частни бизнес структури.

Вътрешните фактори са липсата на необходимия административен капацитет и наличието на дефицити в управлението на граничната сигурност.²⁷

На първо място са *несъвършенствата на вътрешното национално законодателство*. Традиционно то делегира ексклузивни правомощия по опазването на границата и осъществяването на граничния режим само на конкретна специализирана военна, полицейска или от смесен тип служба. Последниците от тази регламентация е стриктното опазване на компетенциите и трудностите, а често и невъзможността за осъществяване на смесени компетенции заедно с други правоприлагащи органи. Липсата на пълноценна координация и взаимодействие се мултиплицира в липсата на оперативна комуникация и недостатъчност /ограниченост на оперативната информация. Известен е стремежът на специалните служби ревностно да съхраняват и да не споделят помежду си придобитата от тях информация. Много често информационните им масиви съдържат данни, които са необходими на друга полицейска или разузнавателна структура. В резултат на недостатъчното информационно осигуряване анализът на риска е непълен, което става причина за вземане на грешни управленски решения.

На второ място е *неспособността на граничните служби да осигурят безпроблемен добросъвестен трафик и едновременно да спират незаконния трафик и подобряват граничната сигурност*. Дилемата е концептуална. От една страна, ако усилията и вниманието са насочени приоритетно в първата насока, отслабва контрола по предотвратяване на нелегалния трафик и обратното. Проблемът с разрешаване на конфликтната ситуация има две измерения. Първото се отнася до дефицита на предварителна, конкретна и актуална информация за методите, начините и способите, използвани за незаконна дейност. Граничните служби генерират необходимите им данни за управление на граничната сигурност предимно в резултат на собствените си легитимни действия и това обективно ги ограничава в оперативните им действия срещу нелегалната миграция и транснационалната престъпност. Взаимодействието им с други специални и полицейски служби или частни организации или липсва, или е формално, или е инцидентно в конкретни извънредни и кризисни ситуации. Второто измерение засяга мотивацията на персонала. Служителите са стимулирани от ръководителите си за извършване на ефективен, а не на ефикасен контрол. Най-важни за тях са броят на задържаните лица, откритите фалшиви документи, наркотици, укрити лица и др. Отчита се степента на постигане на целите, а не резултатите спрямо положените усилия и вложените ресурси. Този принцип на работа често е в колизия със законовите разпоредби, правила и процедури, регламентиращи дейността и се отразява негативно на репутацията и обществения имидж на граничните служби.

Въпреки очевидната необходимост от усъвършенстване на традиционните гранични дейности, *прилагането на модела за ИГУ става ексклузивен приоритет на политиките за сигурност на държавите след атентатите на 11 септември 2001 г. в САЩ*. Водещи в теоретичното му обосноваване и практическото му приложение са САЩ и Европейският съюз.

Основните инструменти на модела в ЕС са: анализ на риска; Кодекса на шенгенските граници; централизираните информационни системи като Шенгенска информационна система - ШИС, Визова информационна система - ВИС, информационна система за пръстови отпечатъци - Евродак; оперативното сътрудничество, обучението на персонала и европейските специализирани агенции като Фронтекс и Европол. ИГУ се прилага в държавите членки чрез национални стратегии с планове за действие. **Най-значимото предизвикателство** остава

²⁷ Вж. Корнажева, М., 2005

волята за сътрудничество и изграждане на доверие в контекст на все по-ясно очертаващо се многостепенно управление в ЕС на сектор сигурност. Наследството на Студената война изобилства от стереотипи, чието преодоляване е бавен процес на взаимно опознаване и натрупване на критична маса от доказателства за лоялност към общоевропейските ценности.

От синхронна гледна точка третият етап в развитието на политиките за сигурност на границите е възникването на интелигентния подход. Основната му характеристика е преформулирането на традиционното схващане за охрана на границите в т.нар. **умни/интелигентни граници (smart borders)**. По същество практиките на интегрираното управление се допълват с нови инструменти, подходи и действия чрез широкомащабна дигитализация. Прилагането на интелигентния начин за гранична защита е продиктувано основно от двете миграционни кризи в Европа в резултат първо на „Арабската пролет“ през 2011 г. и на войната в Сирия през 2015 г., както и от терористичните атаки в държави-членки на ЕС.

Настъпилите промени са от фундаментално естество – управлението на границите се превръща в управление на идентичността. Интелигентното гранично управление изисква снемане, събиране и анализ на биометрични данни за лицата, желаещи да посетят територията на САЩ и Европейския съюз. Биометричните характеристики и конкретно пръстовите отпечатащи са уникални по физическата си природа за всеки индивид, позволяват автоматизирано разпознаване и поради това са надеждни като носители на специфична информация и на практика са невъзможни за фалшифициране или подправяне.

Само три месеца след терористичните атаки на 11 септември 2001 г. САЩ и Канада подписват Декларация за интелигентна граница (Smart Border Declaration) с план за действие от 30 точки за повишаване на сигурността на съвместната граница. Създава се съвместна Агенция на граничните служби на Канада и американската митническа и гранична защита НЕКСУС (NEXUS) за ускорен граничен контрол на предварително одобрени, ниско рискови пътници, на които се издава специална карта, заместваща паспорта за пътуване между двете страни. За тях са осигурени отделни коридори.²⁸

Американските власти своевременно модернизират своята програма за статуса на посетителите и имигрантите - United States Visitor and Immigrant Status Indicator Technology, известна като US-VISIT²⁹. Първоначално се сканират по два пръстови отпечатаща, но от 2007 г. всичките десет. В началото програмата обхваща само пътници, за които се изисква виза, но от 30.09.2004 г. става задължителна и за тези с безвизов режим. От 2006 г. Държавният департамент издава паспорти с биометрична информация.

През м. март 2013 г. програмата US-VISIT е заменена със Службата за управление на биометрична идентичност - Office of Biometric Identity Management (OBIM)³⁰. Службата предоставя услуги на всички федерални, щатски и местни правителствени агенции, оторизирани за борба с престъпността.

В Европейския съюз въпросът за интелигентни граници - т. нар. Пакет Интелигентни граници (ПИГ), е предложен от Европейската комисия през 2013 г.³¹. Той е продължение на нейното съобщение от 13.02.2008 г. относно подготовката на следващите стъпки за управление на границите в ЕС чрез създаване на Система за влизане/излизане (СВИ) – Entry/Exit System (EES), Програма за регистрирани пътници (ППП) – Registered Traveller Programme (RTP) и промени в Кодекса на Шенгенските граници в допълнение на използваните системи за управление на границите. Предвижда се СВИ да регистрира в електронна база данни часа и мястото на влизане, както и срока на разрешения престой, които да са на разположение на граничния контрол и имиграционните власти. Въвеждането на системата би довело до

²⁸ Вж. по-подробно в сайта на НЕКСУС <https://www.cbsa-asfc.gc.ca/prog/nexus/menu-eng.html>

²⁹ Вж. брошурата на US-VISIT на сайт https://www.dhs.gov/xlibrary/assets/usvisit/usvisit_edu_10-finger_print_consumer_friendly_content_1400_words.pdf

³⁰ Вж. H.R.5206 - Office of Biometric Identity Management Authorization Act of 2018.

³¹ Вж. Подготовка на следващите стъпки в управлението на границите в Европейския съюз, Съобщение на Комисията, 13 февруари 2008 г.

премахване на поставянето на гранични печати в паспортите чрез електронна регистрация в базата данни.

През 2015 г. Европейската комисия публикува за обществено обсъждане проекта за интелигентни граници, включително и предложенията за неговото регламентиране и съобразно направените препоръки прие на 06.04.2016 г. преработено законодателно предложение – регламент за създаване на СВИ и за изменение на Шенгенския граничен кодекс. Предложението за ПРП отпада от проекта.

Според подготвеното законодателство Системата ва влизане/излизане би трябвало да се прилага от 2022 г.³² на външните граници от страните-членки, прилагащи изцяло достиженията на Шенгенското право спрямо гражданите на трети страни, допуснати за краткосрочен престой и такива, на които е отказано влизане за краткосрочен престой. Тя ще включва в софтуера си автоматичен калкулатор за изчисляване на ограничението от 90 дни в рамките на всеки 180-дневен период. Ще се записват и обработват буквено-цифрови и биометрични данни, което е мотивирано главно за целите на подобряване на управлението на външните граници, предотвратяването на незаконната миграция и улесняването на управлението на миграционните потоци. Изтъква се, че това е особено важно за идентификация на граждани на трети страни, намиращи се на територията на Съюза без документи за пътуване, което е обичайно за незаконните мигранти. Изисква се да се регистрират по възможност четири пръстови отпечатъка от пътник, но техният брой може да бъде намален при използване на дигиталното изображение на лицето му - портретна снимка. Данните за лица, които са спазили разрешения им срок, ще се съхраняват три години, а на тези, които не са напуснали в рамките на разрешения срок ще се съхраняват пет години. Подробно е описана техническата архитектура на системата, критериите за въвеждане на данните, нейната оперативна съвместимост с ВИС, нивата и условията за достъп, опазването на личните данни, възможността данните в нея да се ползват от правоприлагащите органи и др. Системата предлага и уеб-услуга за граждани на трети страни, чрез която могат да проверят дали отговарят на условията за издаване на виза или да получат информация за оставащият им разрешен престой.³³ С Регламента за създаване на СВИ се създава Комитет за интелигентни граници, който да подпомага ЕК.³⁴ Достъп до СВИ ще имат националните правоприлагащи органи и Европол, но не и тези, работещи в областта на убежището – при тях е предвидена възможност за ползване на данни от системата при определени условия.

С Решение за изпълнение (ЕС) 2019/326 на Комисията от 25.02.2019 г. се определят мерки за въвеждане на данните в СВИ в съответствие с Регламент (ЕС) 2017/2226³⁵. Според него данните, които се въвеждат се групират в две категории: лично досие и записи за влизане/излизане. Личното досие ще съдържа буквено-цифрови данни – фамилно и собствено име; трибуквен код на държавата, издала документа за пътуване; трибуквен код на държавата, издала визовия стикер; граничният пункт, който е разрешил влизането; различни знаци за статута на гражданина на трета страна – член на семейство на гражданин на Съюза, за прилагане на национална програма за улесняване и др., както и биометричните данни на лицето – задължителна портретна снимка и пръстови отпечатъци.

Критичните становища на редица европейски институции и неправителствени организации са показателни за проблемите, свързани с въвеждането на Системата в действие. Например, Европейският надзорен орган по защита на данните (ЕНОЗД)/European Data Protection Supervisor (EDPS)³⁶ изразява загриженост за правата и свободите на гражданите на трети страни и препоръчва увеличаване на защитата на данните. Сдружението на граждански и правозащитни организации в Европа EDRI - European Digital Rights, отбелязва, че мащабното

³² European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) носи отговорността за разработване и управляване на системата.

³³ Вж. Регламент (ЕС) 2017/2226 от 30.11.2017 г.

³⁴ Пак там, чл. 68.

³⁵ Вж. Решение (ЕС) 2019/326, 25 февруари 2019 г.

³⁶ Вж. Summary of the Opinion of the European Data Protection Supervisor on the proposal for a Regulation on the eu-LISA, 2017

събиране на биометрични данни е непропорционално на целите.³⁷ Агенцията на Европейския съюз за основните права – European Union Agency for Fundamental Rights (FRA) предупреждава за несъразмерните последици за правата на мигрантите и рисковете при незаконен достъп и ползване на личните им данни в поредица от публикации от 2015 до 2018 г.³⁸. Неправителствената организация в обществена полза Statewatch посочва, че „свободата“ в Пространството за свобода, сигурност и правосъдие на ЕС е просто дума, когато се отнася до граничен контрол³⁹.

Основното предизвикателство пред интелигентния начин за управление на границите очевидно се състои в създаването на устойчиви и надеждни технологични и мултимодални платформи за придобиване, използване и съхранение на биометричната информация, позволяващи повишаване на граничната сигурност и същевременно осигуряващи бързо и безпроблемно движение на законния трафик със задължителното условие за **спазване на основните човешки права** и защитата на личното пространство и личните данни. По-надолу в изложението ще посочим такива аргументи предвид новостта на технологията за разпознаване на лица, както и липсата на опит и подробни проучвания за въздействието ѝ.

Както при други широкомащабни информационни системи на ЕС, ясна и детайлна правна рамка трябва да регулира внедряването и използването на технологии за разпознаване на лица. Определянето кога обработката на изображения на лицето е необходима и пропорционална (на риска) трябва да зависи не само от целта, но и от наличието на защита на индивидите от възможни негативни последици от автоматизираната обработка. Трябва да се прави разлика между (1) обработката на изображения на лицето с цел проверка, когато се сравняват две изображения на лицето, за да се провери дали те принадлежат на едно и също лице; и (2) тяхната обработка за целите на идентификацията, когато изображение на лицето се сравнява с изображения на лица на наблюдавани/търсени индивиди. Във втория случай рискът от нарушение на основните права е по-висок и тестът за необходимост и пропорционалност трябва да бъде по-стриктен.

Така наречените „технологии за разпознаване на лица на живо“ - когато изображенията на лицето се извличат от видеокамери, разположени в публични пространства - са особено предизвикателство. Те предизвикват страхове от силен дисбаланс между властта на държавата и индивида. Като се има предвид, че хората може да не са наясно, че изображението на лицето им е съпоставено с това на лица от списък за наблюдение и като се има предвид по-високата честота на грешки в сравнение със ситуации при контролирана среда (като летище или полицейско управление), тяхното използване трябва да остане изключително рядко. То трябва да бъде строго ограничено до борба с тероризма и други форми на тежки престъпления или до разкриване на изчезнали хора и жертви на престъпления.

Когато изображенията на лицето се извличат от видеокамери, разположени в обществени зони, оценката за необходимостта и пропорционалността се отнася до това къде са поставени камерите. Има разлика между спортно или културно събитие и събития, при които хората упражняват едно от основните си права. Разполагането на технологии за разпознаване на лица по време на демонстрации може да генерира ефект, при който хората се чувстват принудени да се въздържат от законно упражняване на свободата на събиране и сдружаване поради страх от негативните последици, които могат да последват. Трудно е да си представим ситуации, при които внедряването на технологии за разпознаване на лица върху хора, участващи в демонстрация, може да е необходимо и пропорционално.

Технологията за разпознаване на лица никога не дава окончателен резултат, а само вероятност две изображения на лица да се отнасят до един и същ човек. По този начин в контекста на правоприлагането може да се допусне грешка. Когато се внедрява технологията, рисковете от неправилно обозначаване на хора като потенциални престъпници трябва да бъдат

³⁷Вж. Berthélémy, Chloé, 2021

³⁸ Вж. Borders and information systems, 2015-2018 <https://fra.europa.eu/en/themes/borders-and-information-systems>

³⁹Вж. Jones, C., 2014

сведени до минимум, а за всеки, който е спрял в резултат на технологията, трябва да се отчита правото на достойнство.

Публичните власти обикновено разчитат на частни компании за набавяне и внедряване на технологията. Индустрията и научноизследователската общност могат да играят важна роля в разработването на технически решения, които насърчават зачитането на основните права, включително защитата на личните данни. Затова съображенията относно основните права трябва да бъдат включени в техническите спецификации и договорите. Директивата за обществените поръчки на ЕС (2014/24/ЕС) въведе изискване към държавите-членки за социална отговорност. Следвайки духа на директивата, ЕС и държавите-членки биха могли да приложат подобен подход при набавяне на технология за разпознаване на лица и възлагане на изследвания, като поставят основните права и по-специално изискванията за защита на данните и недискриминация в центъра на всички технически спецификации.

Възможни мерки са задължително изискване за включване на експерти по защита на данните и специалисти по правата на човека в екипите, работещи по развитието на технологията. Освен това, техническите спецификации могат да се позовават на стандарти за високо качество, за да се сведат до минимум процентите на фалшиво идентифициране и неблагоприятно въздействие върху пола, етническата принадлежност и възрастта. Оценка на въздействието на технологията върху основните права е основен инструмент. Публичните власти трябва да оценят изчерпателно всички засягани права. За да могат да го направят, те трябва да получат цялата необходима информация от индустрията. Търговските тайни или съображения за поверителност не трябва да възпрепятстват тези усилия.

В светлината на непрекъснато развиващата се технология, намесата в основните права не е лесно да се предскаже. По тази причина е нужно наблюдение от независими надзорни органи. Хартата за защита на личните данни изисква надзор върху обработката на данни от независим орган. За да се предотвратят нарушенията на основните права и ефективно да се подкрепят хората, чиито основни права са засегнати от технологията за разпознаване на лица, надзорните органи трябва да разполагат с достатъчно правомощия, ресурси и опит.

ЗАКЛЮЧЕНИЕ

В тази разработка очертахме три фази в еволюцията на политики за сигурност на границите – традиционно управление, интегрирано управление и управление на умни граници. Посочихме, че при тази еволюция се надграждат управленски функции.

Днес управлението на сигурността на границите се характеризира с нараснала сложност и предизвикателства, произтичащи от потенциала на дигиталните технологии. Дебатът върху дилемата сигурност или свобода придоби нова актуалност. Той разкри и възможност **сигурността и свободата да се разглеждат като взаимодопълващи се ценности чрез инкорпориране на политики за правата на човека в политиките за разработването и прилагането на технологии за събиране и използване на биометрични данни**. Това обаче винаги ще зависи от качеството на демокрацията и прилагането на принципа за върховенство на правото в ЕС и в държавите членки на ЕС.

REFERENCES

A Regulation on the EU-LISA (2017).// https://edps.europa.eu/sites/default/files/publication/17-11-16_eu_lisa_opinion_summary_en.pdf

Albrow, M. Introduction (1990) //M. Albrow and E. King (Eds.), Globalisation, Knowledge and Society. London: Sage

Andreas, P. (2003) Redrawing the Line: Borders and Security in the Twenty-First Century// International Security, Vol. 28, No. 2 (Fall, 2003), pp. 78-111

Berthélémy, C. (2021). Eurodac database repurposed to surveil migrants.// <https://edri.org/our-work/eurodac-database-repurposed-to-surveil-migrants/>

Borders and Information Systems (2015-2018)// <https://fra.europa.eu/en/themes/borders-and-information-systems>

European Security Strategy - A secure Europe in a better world, Council of EU (2009)// <https://www.consilium.europa.eu/en/documents-publications/publications/european-security-strategy-secure-europe-better-world/>

For Secure, Efficient and Future-Proof Air, Land and Sea Borders.//<https://www.secunet.com/en/solutions-services/state-security-and-tasks-of-public-authorities/border-control/>

Internal Security Strategy for the European Union - Towards a European Security Model (2010). //Council of the European Union, General Secretariat, EU Schengen Catalogue// <https://www.consilium.europa.eu/en/documents-publications/publications/internal-security-strategy-european-union-towards-european-security-model/>

Jones, C., (2014) Smart borders: fait accompli? Statewatch Analysis.// <https://www.statewatch.org/media/documents/analyses/no-253-smart-borders.pdf>

Kornazheva, M. 2005. Border Governance Policies: Bulgarian Experience on the Eve of EU Membership. // Proceedings of University of Ruse, 2005 (Оригинално заглавие Корнажева, М. Политики при управление на границите: български опит в процеса на подготовка за членство в ЕС. // Научни трудове на Русенски университет. Том 44, серия 5.3. Европеистика. Русе, 2005, с. 138 -166, ISSN:1311-3321)

Morag, N. (2020) “Border Management in Europe: Is the Paradigm Evolving?” Homeland Security Affairs 16, Article 1// www.hsaj.org/articles/15835

Summary of the Opinion of the European Data Protection Supervisor on the proposal for The Commission, Preparing the next steps in border management in the European Union, 13 February 2008. COM (2008)69 Eue // <https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vikqhmb7zk>

U.S., Canada sign 'smart border' declaration. CNN.com. OTTAWA, Ontario: CNN. December 13, 2001. Retrieved 25 September 2020 // <http://edition.cnn.com/2001/US/12/12/rec.canada.border/>

U.S. - Canada Smart Border/30 Point Action Plan Update. Georgewbush-whitehouse.archives.gov. Retrieved 25 September 2020// <https://georgewbush-whitehouse.archives.gov/news/releases/2002/12/20021206-1.html>